(U) SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, SUBMITTED BY THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE

Reporting Period: December 1, 2015 – May 31, 2016

August 2017

[redacted]

(U) SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, SUBMITTED BY THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE

August 2017

TABLE OF CONTENTS

(U) Fact Sheet 3

(U) Executive Summary 5

(U) Section 1: Introduction 6

(U) Section 2: Oversight of the Implementation of Section 702 8

- (U) I. Joint Oversight of NSA 9
- (U) II. Joint Oversight of CIA 11
- (U) III. Joint Oversight of FBI 12
- (U) IV. Joint Oversight of NCTC 15
- (U) V. Interagency/Programmatic Oversight 16
- (U) VI. Training 16

(U) Section 3: Trends in Section 702 Targeting and Minimization 17

- (U) I. Trends in NSA Targeting and Minimization 17
- (U) II. Trends in FBI Targeting 21
- (U) III. Trends in CIA Minimization 23

(U) Section 4: Compliance Assessment – Findings 27

- (U) I. Compliance Incidents – General 27
- (U) II. Review of Compliance Incidents – NSA Targeting and Minimization Procedures 34
- (U) III. Review of Compliance Incidents – CIA Minimization Procedures 48
- (U) IV. Review of Compliance Incidents – FBI Targeting and Minimization Procedures 48
- (U) V. Review of Compliance Incidents – Provider Errors 50

(U) Section 5: Conclusion 51

(U) Appendix A A-1

(When this 2-Page Fact Sheet is Separated from this Assessment, this Fact Sheet is Unclassified.)

(U) FACT SHEET

(U) Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (FISA) Joint Assessments

(U) This Fact Sheet provides an overview of the *Semiannual Assessments of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*. These assessments are commonly referred to as "Joint Assessments," and are submitted by the Attorney General and the Director of National Intelligence (DNI). As of August 2017, sixteen joint assessments have been submitted.

(U) Joint Assessment Basics:

- *(U) Why is the Joint Assessment required?* The FISA Amendments Act of 2008 (50 U.S.C. § 1881(l)(1)) requires the Attorney General and the DNI to assess compliance with certain procedures and guidelines issued pursuant to FISA Section 702.
- *(U) What period is covered by a Joint Assessment?* Each Joint Assessment covers six-month periods: December 1 – May 31 or June 1 – November 30.
- *(U) Who receives it?* Each Joint Assessment is submitted to the Foreign Intelligence Surveillance Court (FISC) and relevant congressional committees.
- *(U) What is being assessed?* The Attorney General and the DNI must jointly assess the government's compliance with FISC-approved "targeting procedures" and "minimization procedures."

(U) Highlights from 16th Joint Assessment:

- *(U) No intentional violations*. Consistent with previous Joint Assessments, no instances of intentional circumvention or violation of those procedures were found.
- *(U) Continued focused efforts to implement Section 702 in a compliant manner*. The Joint Assessment reports that the agencies continued to implement the procedures in a manner that reflected a focused and concerted effort by Intelligence Community (IC) personnel to comply with the requirements of Section 702.
- *(U) Compliance incident rate remains low*. The compliance incident rate remained low, which is consistent with the compliance incident rate reported for other reporting periods. The majority of incidents were caused by a misunderstanding of the procedures, failure to conduct the required checks, technical issues and inadvertent human errors.

- *(U) What are targeting procedures and minimization procedures?* Section 702 allows for the targeting of (i) non-United States persons (ii) reasonably believed to be located abroad (iii) to acquire foreign intelligence information. To ensure that all three requirements are appropriately met, Section 702 requires targeting procedures. Targeting is effectuated by tasking communications facilities (such as telephone numbers and electronic communications accounts) to U.S. electronic communications service providers. Section 702 also requires minimization procedures to minimize and protect any non-public information of United States persons that may be incidentally collected when appropriately targeting non-United States persons abroad for foreign intelligence information.

(When this 2-Page Fact Sheet is Separated from this Assessment, this Fact Sheet is Unclassified.)

(*When this 2-Page Fact Sheet is Separated from this Assessment, this Fact Sheet is Unclassified.)*

- *(U) What compliance and oversight efforts underlie the Joint Assessment?* Agencies employ extensive compliance measures to implement Section 702 in accordance with procedural, statutory, and constitutional requirements. A joint oversight team consisting of experts from the Department of Justice (DOJ) and the Office of the Director of National Intelligence (ODNI) oversee these measures. Each incident of non-compliance (i.e. compliance incident) is documented, reviewed by the joint oversight team, remediated, and reported to the FISC and relevant congressional committees. The Joint Assessment summarizes trends and assesses compliance (including calculating the compliance incident rate for the relevant reporting period) and may include recommendations to help prevent compliance incidents or increase transparency.

- *(U) What government agencies are involved with implementing Section 702?* The National Security Agency (NSA), the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA) and the National Counterterrorism Center (NCTC). Each Joint Assessment discusses how these agencies implement the authority.

- *(U) Why is the Joint Assessment classified?* The Joint Assessment is classified to allow us to provide the congressional oversight committees a complete assessment of the Section 702 program while at the same time protecting sources and methods. They are carefully redacted for public release in the interest of transparency.

- *(U) What is the format of the Joint Assessment?* The Joint Assessment generally contains an executive summary, five sections, and an appendix. New with the 16th Joint Assessment is the additional appendix containing this fact sheet about the joint assessments. Sections 1 and 5 provide an introduction and conclusion. Section 2 details internal compliance efforts by the agencies that implement Section 702, interagency oversight, training efforts and efforts to improve the implementation of Section 702. Section 3 compiles and presents data acquired from compliance reviews of the targeting procedures and minimization procedures. Section 4 describes compliance trends. The Joint Assessment describes the extensive measures undertaken by the government to ensure compliance with court-approved targeting and minimization procedures; to accurately identify, record and correct errors; to take responsive actions to remove any erroneously obtained data; and to minimize the chances that mistakes will re-occur.

- *(U) What are the types of compliance incidents discussed?* Generally, the Joint Assessment groups incidents into six categories. Categories 1-4 (tasking incidents, detasking incidents, notification delays and documentation errors) discuss non-compliance with targeting procedures. Category 5 discusses incidents of non-compliance with minimization procedures such as erroneous queries of 702 information using U.S. person identifiers. Finally, category 6 is a catch-all category for incidents that do not fall into one of the other five categories. The actual number of the compliance incidents is classified; however, the percentage breakdown of those incidents is unclassified and reported in the Joint Assessment. Additionally, because Section 702 collection occurs with the assistance of U.S. electronic communications service providers who receive a Section 702(h) directive, the Joint Assessment includes a review of any compliance incidents by such service providers.

(*When this 2-Page Fact Sheet is Separated from this Assessment, this Fact Sheet is Unclassified.)*

(U) Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence

August 2017

Reporting Period: December 1, 2015 – May 31, 2016

(U) EXECUTIVE SUMMARY

(U) The FISA Amendments Act of 2008 (hereinafter "FAA") requires the Attorney General and the Director of National Intelligence (DNI) to assess compliance with certain procedures and guidelines issued pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 *et seq*., as amended, (hereinafter "FISA" or "the Act") and to submit such assessments to the Foreign Intelligence Surveillance Court (FISC) and relevant congressional committees at least once every six months. Section 702 authorizes, subject to restrictions imposed by the statute and required targeting and minimization procedures, the targeting of non-United States persons reasonably believed to be located outside the United States in order to acquire foreign intelligence information. The present assessment sets forth the sixteenth joint compliance assessment of the Section 702 program. This assessment covers the period from December 1, 2015 through May 31, 2016 (hereinafter the "reporting period") and accompanies the Semiannual Report of the Attorney General Concerning Acquisitions under Section 702 of the Foreign Intelligence Surveillance Act as required by Section 707(b)(1) of FISA (hereinafter "the Section 707 Report"). The Department of Justice submitted the Section 707 Report on September 1, 2016; it covers the same reporting period as the Joint Assessment.

(U) This Joint Assessment is based upon the compliance assessment activities that have been jointly conducted by the Department of Justice's National Security Division (NSD) and the Office of the Director of National Intelligence (ODNI).

(U) This Joint Assessment finds that the agencies have continued to implement the procedures and follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702. The personnel involved in implementing the authorities are appropriately focused on directing their efforts at non-United States persons reasonably believed to be located outside the United States for the purpose of acquiring foreign intelligence information. Processes are in place to implement these authorities and to impose internal controls for compliance and verification purposes. However, given the complexities of implementing this authority a certain number of compliance incidents will always be present. Keeping compliance incidents to a relatively small number that have small implications is a goal of those implementing this authority and those overseeing it. Specifically, the compliance incidents that occurred during this reporting period represent a very small percentage (0.45%) of the overall collection activity. This represents a decrease from the last Joint Assessment's rate of 0.53% and still remains well below 1%. Individual incidents, however, can have broader implications, as further discussed herein and in the Section 707 Report. Based upon a review of these compliance incidents, the joint oversight team believes that none of these incidents represent

an intentional attempt to circumvent or violate the Act, the targeting or minimization procedures, or the Attorney General's Acquisition Guidelines.

(U) SECTION 1: INTRODUCTION

(U) The FISA Amendments Act of 2008 (hereinafter, "FAA") requires the Attorney General and the Director of National Intelligence (DNI) to assess compliance with certain procedures and guidelines issued pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 *et seq.*, as amended (hereinafter, "FISA" or "the Act"), and to submit such assessments to the Foreign Intelligence Surveillance Court (FISC) and relevant congressional committees at least once every six months. As required by the Act, a team of oversight personnel from the Department of Justice's National Security Division (NSD) and the Office of the Director of National Intelligence (ODNI) have conducted compliance reviews to assess whether the authorities under Section 702 of FISA (hereinafter, "Section 702") have been implemented in accordance with the applicable procedures and guidelines, discussed herein. This report sets forth NSD and ODNI's sixteenth joint compliance assessment under Section 702, covering the period December 1, 2015 through May 31, 2016 (hereinafter, the "reporting period").[1]

(U) Section 702 requires that the Attorney General, in consultation with the DNI, adopt targeting and minimization procedures, as well as guidelines. A primary purpose of the guidelines is to ensure compliance with the limitations set forth in subsection (b) of Section 702, which are as follows:

> An acquisition authorized under subsection (a)—
>
> (1) may not intentionally target any person known at the time of acquisition to be located in the United States;
> (2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;
> (3) may not intentionally target a United States person reasonably believed to be located outside the United States;
> (4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and
> (5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

The Attorney General's Guidelines for the Acquisition of Foreign Intelligence Information Pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended (hereinafter "the Attorney

[1] (U) This report accompanies the Semiannual Report of the Attorney General Concerning Acquisitions under Section 702 of the Foreign Intelligence Surveillance Act, which was previously submitted on September 1, 2016, as required by Section 707(b)(1) of FISA (hereafter Section 707 Report). This sixteenth Joint Assessment covers the same reporting period as the sixteenth Attorney General's Section 707 Report.

General's Acquisition Guidelines") were adopted by the Attorney General, in consultation with the DNI, on August 5, 2008.

(U) During this reporting period, the Government acquired foreign intelligence information under Attorney General and DNI authorized Section 702(g) certifications that targeted non-United States persons reasonably believed to be located outside the United States in order to acquire different types of foreign intelligence information.[2] Three agencies are primarily involved in implementing Section 702: the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), and the Central Intelligence Agency (CIA). An overview of how these agencies implement the authority appears in Appendix A of this assessment. The other agency involved in implementing Section 702 is the National Counterterrorism Center (NCTC), which currently has a limited role, as reflected in the "Minimization Procedures Used by NCTC in connection with Information Acquired by FBI pursuant to Section 702 of FISA, as amended."[3]

(U) Section Two of this Joint Assessment provides a comprehensive overview of oversight measures the Government employs to ensure compliance with the targeting and minimization procedures, as well as the Attorney General's Acquisition Guidelines. Section Three compiles and presents data acquired from the joint oversight team's compliance reviews in order to provide insight into the overall scope of the Section 702 program, as well as trends in targeting, reporting, and the minimization of United States person information. Section Four describes compliance trends. All of the specific compliance incidents for the reporting period have been previously described in detail in the Section 707 Report. As with the prior Joint Assessments, some of those compliance incidents are analyzed here to determine whether there are patterns or trends that might

[2] [redacted]

[3] (U) Under these limited minimization procedures, during this reporting period, NCTC was not authorized to receive unminimized Section 702 data. Rather, these procedures recognize that, in light of NCTC's statutory counterterrorism role and mission, NCTC has been provided access to certain FBI systems containing *minimized* Section 702 information, and prescribe how NCTC is to treat that information. For example, because NCTC is not a law enforcement agency, it may not receive disseminations of Section 702 information that is evidence of a crime, but which has no foreign intelligence value; accordingly, NCTC's minimization procedures require in situations in which NCTC personnel discover purely law enforcement information with no foreign intelligence value in the course of reviewing minimized foreign intelligence information that the NCTC personnel either purge that information (if the information has been ingested into NCTC systems) or not use, retain, or disseminate the information (if the information has been viewed in FBI systems). Subsequent to this reporting period, NCTC was authorized by the FISC to receive unminimized Section 702 data. Specifically, in an opinion issued by the FISC on April 26, 2017, the FISC approved new minimization procedures for NCTC (2016 NCTC Minimization Procedures). The 2016 NCTC Minimization Procedures reflect that NCTC may now receive unminimized Section 702 information.

indicate underlying causes that could be addressed through additional measures, and to assess whether the agency involved has implemented processes to prevent recurrences. Finally, this Joint Assessment contains two Appendices. Appendix A, contained in previous joint assessments as well, details how each agency implements Section 702 and includes a general description of the oversight at each agency.

(U) In summary, the joint oversight team finds that the agencies have continued to implement the procedures and follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702 during this reporting period. As in the prior Joint Assessments, the joint oversight team has not found indications in the compliance incidents that have been reported or otherwise identified of any intentional or willful attempts to violate or circumvent the requirements of the Act. The number of compliance incidents remains small, particularly when compared with the total amount of targeting and collection activity. In its ongoing efforts to reduce the number of future compliance incidents, the Government will continue to focus on measures to improve (a) inter and intra-agency communication, (b) training, and (c) systems used in the handling of Section 702-acquired communications, including those systems needed to ensure that appropriate purge practices are followed and that certain disseminated reports are withdrawn as required. Further, the joint oversight team will also continue to monitor agency practices to ensure appropriate remediation steps are taken to prevent, whenever possible, reoccurrences of the types of compliance incidents discussed herein and in the Section 707 Report. As appropriate, this Joint Assessment provides updates on these on-going efforts.

(U) SECTION 2: OVERSIGHT OF THE IMPLEMENTATION OF SECTION 702

(U) The implementation of Section 702 is a multi-agency effort. As described in detail in Appendix A, NSA and FBI each acquire certain types of data pursuant to their own Section 702 targeting procedures. NSA, FBI, and CIA[4] each handle Section 702-acquired data in accordance with their own minimization procedures.[5] There are differences in the way each agency implements its procedures resulting from unique provisions in the procedures themselves, differences in how these agencies utilize Section 702-acquired data, and efficiencies from using preexisting systems to implement Section 702 authorities. Because of these differences in practice and procedure, there are corresponding differences in each agency's internal compliance programs and in the external NSD and ODNI oversight programs.

[4] (U) As discussed herein, CIA receives Section 702-acquired data from NSA and FBI.

[5] (U) Each agency's targeting and minimization procedures are approved by the Attorney General and reviewed by the Foreign Intelligence Surveillance Court. In 2015, the DNI released, in redacted form, NSA's, FBI's, and CIA's 2014 minimization procedures on ODNI's *IC on the Record* website as part of its SIGINT Intelligence Reform 2015 Anniversary Report (hereinafter the "2015 Anniversary Report"). On August 11, 2016, the DNI released, in redacted form, NSA's, FBI's, and CIA's (as well as NCTC's) 2015 minimization procedures on ODNI's *IC on the Record* website as part of DNI's commitment to the IC's Principles of Transparency. On May 11, 2017, the DNI released, in redacted form, NSA's, FBI's, CIA's, and NCTC's 2016 minimization procedures and NSA's and FBI's 2016 targeting procedures on *IC on the Record*.

(U) A joint oversight team has been assembled to conduct compliance assessment activities, consisting of members from NSD, ODNI's Office of Civil Liberties, Privacy and Transparency (ODNI CLPT), ODNI's Office of General Counsel (ODNI OGC), and ODNI's Office of the Deputy Director for Intelligence Integration/Mission Integration Division (ODNI DD/II/MID). The team members play complementary roles in the review process. The following describes the oversight activities of the joint oversight team, the results of which, in conjunction with the internal oversight conducted by the reviewed agencies, provide the basis for this Joint Assessment.

(U) I. Joint Oversight of NSA

(U) Under the process established by the Attorney General and Director of National Intelligence's certifications, all Section 702 targeting is initiated pursuant to the NSA's targeting procedures. Additionally, NSA is responsible for conducting post-tasking checks of all Section 702-tasked communication facilities[6] (also referred to as selectors) once collection begins. NSA must also minimize its collection in accordance with its minimization procedures. Each of these responsibilities is detailed in Appendix A. Given its central role in the Section 702 process, NSA has devoted substantial oversight and compliance resources to monitoring its implementation of the Section 702 authorities. NSA's internal oversight and compliance mechanisms are further described in Appendix A.

(U) NSD and ODNI's joint oversight of NSA's implementation of Section 702 consists of periodic compliance reviews, which the NSA targeting procedures require,[7] as well as the investigation and reporting of specific compliance incidents. During this reporting period, NSD and ODNI conducted the following onsite reviews at NSA:

Figure 1: (U) NSA Reviews

Date of Review	Taskings/Minimization Reviewed
February 26, 2016	December 1, 2015 – January 31, 2016
April 29, 2016	February 1, 2016 – March 31, 2016
June 17, 2016	April 1, 2016 – May 31, 2016

(U) Reports for each of these reviews document the relevant time period of the review, the number and types of communication facilities tasked, and the types of information that NSA relied upon, as well as provide a detailed summary of the findings for that review period. These reports have been provided to the congressional committees with the Section 707 Report, as required by Section 707(b)(1)(F) of FISA.

[6] (U) Section 702 authorizes the targeting of non-United States persons reasonably believed to be located outside the United States. This *targeting* is effectuated by *tasking* communication facilities (i.e. selectors), including but not limited to telephone numbers and electronic communications accounts, to Section 702 electronic communication service providers. The oversight review process, which is described within this joint assessment, applies to the targeting of every communication facility regardless of the type of facility. A fuller description of the Section 702 targeting process may be found in the Appendix. This assessment uses the terms facilities and selectors interchangeably and is not attempting to make a substantive distinction between the two terms.

[7] (U) NSA's targeting procedures require that the onsite reviews occur approximately every two months.

(U) The joint oversight review process for NSA targeting begins well before the onsite review. Prior to each onsite review, NSA electronically sends the tasking record (known as a tasking sheet) for *each* facility tasked during the review period to NSD and ODNI. Members of the joint oversight team initially review the tasking sheets, with ODNI team members sending any questions they may have concerning the tasking sheets to NSD, who then prepare a detailed report of the findings, including any questions and requests for additional information. NSD shares this report with the ODNI members of the joint oversight team. During this initial review, the joint oversight team determines whether the tasking sheets meet the documentation standards required by NSA's targeting procedures and provide sufficient information for the reviewers to ascertain the basis for NSA's foreignness determinations. For those tasking sheets that, on their face, meet the standards and provide sufficient information, no further supporting documentation is requested. The joint oversight team then identifies the tasking sheets that did not provide sufficient information and requests additional information.

(U) During the onsite review, the joint oversight team examines the cited documentation underlying these identified tasking sheets, together with NSA Signals Intelligence Directorate (SID) Oversight and Compliance personnel, NSA attorneys, and other NSA personnel as required. The joint oversight team works with NSA to answer questions, identify issues, clarify ambiguous entries, and provide guidance on areas of potential improvement. Interaction continues following the onsite reviews in the form of electronic and telephonic exchanges to answer questions and clarify issues.

(U) The joint oversight team also reviews NSA's minimization of Section 702-acquired data. NSD reviews all of the serialized reports (with ODNI reviewing a sample) that NSA has disseminated and identified as containing Section 702-acquired United States person information. The team also reviews a sample of serialized reports that NSA has disseminated and identified as containing Section-702 acquired *non*-United States person information. NSD and ODNI also review a sample of NSA disseminations to certain foreign government partners made outside of its serialized reporting process. These disseminations consist of information that NSA has evaluated for foreign intelligence and minimized, but which may not have been translated into English.

(U) With respect to queries of Section 702-acquired *content* using a United States person identifier, the joint oversight team reviews all approved United States person identifiers to ensure compliance with the minimization procedures.[8] For each approved identifier, NSA also provides information detailing why the proposed use of the United States person identifier would be reasonably likely to return foreign intelligence information, the duration for which the United States person identifier has been authorized to be used as a query term, and any other relevant information. In addition, with respect to queries of Section 702-acquired *metadata* using a United States person identifier, NSA's internal procedures require that NSA analysts document the basis for each

[8] (U) On May 2, 2016, the DNI publicly released ODNI's third annual *Transparency Report[s]: Statistical Transparency Report Regarding Use of National Security Authorities* for calendar year 2015 (hereafter the *2015 Transparency Report*). Pursuant to reporting requirements proscribed by the USA FREEDOM Act (see 50 U.S.C. § 1873(b)(2)(A)), the *2015 Transparency Report* provided the "estimated number of search terms concerning a known U.S. person used to retrieve the unminimized contents of communications obtained under Section 702" (emphasis added) for the entire calendar year of 2015. On May 2, 2017, the DNI publicly released ODNI's fourth such statistical transparency report, which provided these statistics pertaining to calendar year 2016.

metadata query prior to conducting the query. NSD reviews the documentation for 100% of the metadata queries that NSA provides to NSD.[9]

(U) Additionally, the joint oversight team investigates and reports incidents of noncompliance with the NSA targeting and minimization procedures, as well as with the Attorney General Acquisition Guidelines. While some of these incidents may be identified during the reviews, most are identified by NSA analysts or by NSA's internal compliance program. NSA is also required to report certain events that may not be incidents of non-compliance. For example, NSA is required to report *all* instances in which Section 702 acquisition continued while a targeted individual was in the United States, whether or not NSA had any knowledge of the target's travel to the United States.[10] The purpose of such reporting is to allow the joint oversight team to assess whether a compliance incident has occurred and to confirm that any necessary remedial action is taken. Investigations of all of these incidents sometimes result in requests for supplemental information. All compliance incidents identified by these investigations are reported to the congressional committees in the Section 707 Report and to the FISC.

(U) II. Joint Oversight of CIA

(U) As further described in detail in Appendix A, although CIA does not directly engage in targeting or acquisition, it does nominate potential Section 702 targets to NSA. Because CIA nominates potential Section 702 targets to NSA, the joint oversight team conducts onsite visits at CIA and the results of these visits are included in the bimonthly NSA review reports discussed above. CIA has established internal compliance mechanisms and procedures to oversee proper implementation of its Section 702 authorities.

(U) The onsite reviews also focus on CIA's application of its Section 702 minimization procedures. For this reporting period, NSD and ODNI conducted the following onsite reviews at CIA:

Figure 2: (U) CIA Reviews

Date of Visits	Minimization Reviewed
March 10 and 16, 2016	December 1, 2015 – January 31, 2016
May 4 and 6, 2016	February 1, 2016 – March 31, 2016
June 22 and 24, 2016	April 1, 2016 – May 31, 2016

[9] (U) Also pursuant to reporting requirements proscribed by the USA FREEDOM Act (see 50 U.S.C. § 1873(b)(2)(B)), the 2015 Transparency Report provided the "estimated number of queries concerning a known U.S. person used to retrieve the unminimized noncontents [(i.e. metadata)] information obtained under Section 702" (emphasis added) for the entire calendar year of 2015. On May 2, 2017, the DNI publicly released ODNI's fourth such statistical transparency report, which provided these statistics pertaining to calendar year 2016.

[10] (U) If NSA had no prior knowledge of the target's travel to the United States and, upon learning of the target's travel, immediately "detasked" (i.e. stopped collection against) the target's facility, as is required by NSA's targeting procedures, then the collection while the target was in the United States would not be considered a compliance incident under NSA's targeting procedures, although the collection would generally be subject to purge under the applicable minimization procedures. The joint oversight team carefully considers and, where appropriate, obtains additional facts regarding every reported detasking decision to ensure that NSA's collection and detasking complied with its targeting and minimization procedures.

Reports for each of these reviews have previously been provided to the congressional committees with the Section 707 Report, as required by Section 707(b)(1)(F) of FISA.

(U) As a part of the onsite reviews, the joint oversight team examines documents related to CIA's retention, dissemination, and querying of Section 702-acquired data. The team reviews a sample of communications acquired under Section 702 and identified as containing United States person information that have been minimized and retained by CIA. Reviewers ensure that communications have been properly minimized and discuss with personnel issues involving the proper application of CIA's minimization procedures. The team also reviews all disseminations of information acquired under Section 702 that CIA identified as potentially containing United States person information. NSD and ODNI also review CIA's written foreign intelligence justifications for all queries using United States person identifiers of the content of unminimized Section 702-acquired communications.

~~(S//NF)~~ CIA may receive [redacted][11] unminimized Section 702-acquired communications. Such communications must be minimized pursuant to CIA's minimization procedures. [redacted] as further described in detail in Appendix A, CIA nominates potential Section 702 targets to NSA. [redacted] the joint oversight team conducts onsite visits at CIA to review CIA's original source documentation [redacted] the results of these visits are included in the bimonthly NSA review reports discussed above. CIA has established internal compliance mechanisms and procedures to oversee proper implementation of its Section 702 authorities. These processes are further described in Appendix A.

(U) In addition to the bimonthly reviews, the joint oversight team also investigates and reports incidents of noncompliance with CIA's minimization procedures, the Attorney General Acquisition Guidelines, or other agencies' procedures in which CIA is involved.[12] Investigations are coordinated through the CIA FISA Program Office and CIA's Office of General Counsel (CIA OGC), and when necessary, may involve requests for further information, meetings with CIA legal, analytical, and/or technical personnel, or the review of source documentation. All compliance incidents identified by these investigations are reported to the congressional committees in the Section 707 Report and to the FISC.

(U) III. Joint Oversight of FBI

(U) FBI fulfills various roles in the implementation of Section 702. First, FBI is authorized under the certifications to acquire foreign intelligence information. These acquisitions must be conducted pursuant to FBI's Section 702 targeting procedures.

[11] [redacted]

[12] (U) Insofar as CIA nominates facilities for tasking and reviews content that may indicate that a target is located in the United States or is a United States person, some investigations of possible noncompliance with the NSA targeting procedures can also involve CIA.

~~(S//NF)~~ Second, FBI also provides [redacted] Pursuant to its own authority, FBI is authorized [redacted] from electronic communication service providers by targeting facilities that NSA designates (hereinafter "Designated Accounts"). FBI conveys [redacted] from the electronic communications service providers [redacted] for processing in accordance with the agencies' FISC-approved minimization procedures.

~~(S//NF)~~ Third, [redacted] FBI may receive [redacted] unminimized Section 702-acquired communications. Such communications must be minimized pursuant to FBI's Section 702 minimization procedures. Like CIA, FBI has a process for nominating to NSA new facilities to be targeted pursuant to Section 702.

(U) FBI's internal compliance program and NSD and ODNI's oversight program are designed to ensure FBI's compliance with statutory and procedural requirements for each of these three roles. Each of the roles discussed above, as well as FBI's internal compliance program, are set forth in further detail in Appendix A.

(U) NSD and ODNI generally conduct monthly reviews at FBI Headquarters of FBI's compliance with its targeting procedures and bimonthly reviews at FBI Headquarters of FBI's compliance with its minimization procedures. Reports for each of these reviews have previously been provided to the congressional committees with the Section 707 Report, as required by Section 707(b)(1)(F) of FISA. For this reporting period, onsite reviews at FBI Headquarters were conducted on the following dates:

Figure 3: (U) FBI Reviews

Date of Visit	Targeting and Minimization Reviewed
February 18 and 19, 2016	December 2015 targeting decisions
March 3 and 4, 2016	January 2016 targeting decisions
April 7 and 8, 2016	February 2016 targeting decisions and December 1, 2015 through February 29, 2016, minimization decisions
May 16 and 17, 2016	March 2016 targeting decisions
June 20 and 21, 2016	April 2016 targeting decisions and March 1 through May 31, 2016, minimization decisions
June 21 and 22, 2016	May 2016 targeting decisions

(U) In conducting the targeting review, the joint oversight team reviews the targeting checklist completed by FBI analysts and supervisory personnel involved in the process, together with supporting documentation.[13] The joint oversight team also reviews a sample of other files to

[13] ~~(S//NF)~~ Supporting document includes, among other things [redacted] The joint oversight team reviews every file identified by FBI [redacted]

identify any other potential compliance issues. FBI analysts, supervisory personnel, and attorneys from FBI's Office of General Counsel (FBI OGC) are available to answer questions, and provide supporting documentation. The joint oversight team provides guidance on areas of potential improvement.

(U) At the FBI Headquarters reviews, with respect to minimization, the joint oversight team reviews documents related to FBI's application of its Section 702 minimization procedures. The team reviews a sample of communications that FBI has marked in its systems as both meeting the retention standards and containing United States person information. The team also reviews all disseminations by the relevant FBI Headquarters unit of information acquired under Section 702 that FBI identified as potentially containing non-publicly available information concerning unconsenting United States person information.

(U) In addition to conducting minimization reviews at FBI Headquarters, during this reporting period, NSD continued to conduct minimization reviews at FBI field offices in order to review the retention and dissemination decisions made by FBI field office personnel with respect to Section 702-acquired data. During these field office reviews, NSD reviews a sample of disseminations of information acquired under Section 702 that FBI identified as potentially containing non-publicly available information concerning unconsenting United States persons. At these field office reviews, NSD also reviews a sample of queries, by FBI personnel, in FBI systems that contain raw (i.e. unminimized) FISA-acquired information, including Section 702-acquired information. The purpose for reviewing these queries is to ensure that the queries comply with the requirements in FBI's FISA minimization procedures, including its Section 702 minimization procedures. In addition, as a result of a Court-ordered reporting requirement in the FISC's November 6, 2015 Memorandum Opinion and Order regarding the 2015 FISA Section 702 Certifications,[14] for queries conducted after December 4, 2015, NSD reviews these queries to determine if any such queries were conducted solely for the purpose of returning evidence of a crime. If such a query was conducted, NSD would seek additional information from the relevant FBI personnel as to whether FBI personnel received and reviewed Section 702-acquired information of or concerning a U.S. person in response to such a query. Pursuant to the FISC's opinion and order, such queries must subsequently be reported to the FISC.

(U) As detailed in the attachments to the Attorney General's Section 707 Report, NSD conducted minimization reviews at 15 FBI field offices during this reporting period and reviewed cases involving Section 702-tasked facilities.[15] ODNI joined NSD at a subset of these reviews; ODNI receives written summaries regarding all the reviews from NSD regardless of whether ODNI was in attendance or not. These reviews are further discussed in Section IV below.

---

[14] (U) On April 19, 2016, the DNI, in consultation with the Attorney General, released in redacted form, the FISC's *Order* on the ODNI's public website *IC on the Record*.

~~(S//NF)~~ This November 6, 2015 FISC opinion's formal, but classified, title is [redacted]

[15] ~~(S//NF)~~ During these field office reviews, NSD reviewed [redacted] involving Section 702-tasked facilities, with ODNI reviewing a subset of these cases.

~~(S//NF)~~ Separately, in order to evaluate the FBI's [redacted] acquisition [redacted] and provision of [redacted], the joint oversight team conducts an annual process review with FBI's technical personnel to ensure that these activities comply with applicable minimization procedures. The most recent annual process review, during this reporting period, occurred in April 2016.[16]

~~(S//NF)~~ As further described in detail in Appendix A, FBI nominates potential Section 702 targets to NSA. [redacted] FBI has established internal compliance mechanisms and procedures to oversee proper implementation of its Section 702 authorities. These processes are further described in Appendix A.

(U) The joint oversight team also investigates potential incidents of noncompliance with the FBI targeting and minimization procedures, the Attorney General's Acquisition Guidelines, or other agencies' procedures in which FBI is involved.[17] These investigations are coordinated with FBI OGC and may involve requests for further information, meetings with FBI legal, analytical, and/or technical personnel, or review of source documentation. Compliance incidents identified by these investigations are reported to the congressional committees in the Section 707 Report and to the FISC.

(U) IV. Joint Oversight of NCTC

(U) As noted above, NCTC is also involved in implementing Section 702, albeit in a limited role, as reflected in the "Minimization Procedures Used by NCTC in connection with Information Acquired by the FBI pursuant to Section 702 of FISA, as amended." During this reporting period, under these limited minimization procedures, NCTC was not authorized to receive unminimized Section 702 data, but NCTC had access to certain FBI systems containing minimized Section 702 information. As part of the joint oversight of NCTC to ensure compliance with these procedures, NSD and ODNI conduct reviews of NCTC's access, receipt, and processing of Section 702 information received from FBI. NSD conducted the most recent review review at NCTC for this reporting period in May 2016. As referenced in footnote 3 above, subsequent to this reporting period, NCTC was authorized to receive unminimized Section 702 information. NCTC's processing, retention, and dissemination of such information is subject to its 2016 Minimization Procedures.

[16] ~~(S//NF)~~ A more recent review was conducted in March 2017, which falls outside this Joint Assessment's reporting period.

[17] (U) Insofar as FBI nominates facilities for tasking and reviews content that may indicate that a target is located in the United States or is a United States person, some investigations of possible noncompliance with the NSA targeting procedures can also involve FBI.

(U) V. Interagency/Programmatic Oversight

(U) Because the implementation and oversight of the Government's Section 702 authorities are a multi-agency effort, investigations of particular compliance incidents may involve more than one agency. The resolution of particular compliance incidents can provide lessons learned for all agencies. Robust communication among the agencies is required for each to effectively implement its authorities, gather foreign intelligence, and comply with all legal requirements. For these reasons, NSD and ODNI conduct twice monthly telephone calls and quarterly meetings (in addition to ad hoc calls and meetings on specific topics as needed) with representatives from all agencies implementing Section 702 authorities to discuss and resolve interagency issues affecting compliance with the statute and applicable procedures. Additionally, NSD and ODNI conduct weekly telephone calls with NSA to address outstanding compliance matters, as we work through the process of understanding those matters and reporting incidents to the FISC.

(U) NSD and ODNI's programmatic oversight also involves efforts to proactively minimize the number of incidents of noncompliance. For example, NSD and ODNI have required agencies to demonstrate to the joint oversight team new or substantially revised systems involved in Section 702 targeting or minimization prior to implementation. NSD and ODNI personnel also continue to work with the agencies to review, and where appropriate seek modifications of, their targeting and minimization procedures in an effort to enhance the Government's collection of foreign intelligence information, civil liberties protections, and compliance.

(U) VI. Training

(U) In addition to specific instructions to personnel directly involved in certain incidents of noncompliance discussed in Section 4, the agencies and the joint oversight team have also continued their training efforts to ensure compliance with the targeting and minimization procedures. NSA continued to administer the compliance training course implemented in the prior reporting period. All NSA personnel are required to complete this course on an annual basis in order to gain access to raw Section 702 acquisitions. Additionally, NSA continued providing training on a more informal and ad hoc basis by issuing training reminders and compliance advisories to analysts concerning new or updated guidance to maintain compliance with the Section 702 procedures. These training reminders and compliance advisories are e-mailed to individual analysts and maintained on an internal agency website where personnel can obtain information about specific types of Section 702-related issues and compliance matters. CIA continues to provide regular FISA training at least twice a year to all of the attorneys it embeds with CIA operational personnel. Additionally, CIA has a required training program for anyone handling raw Section 702-acquired data that provides hands-on experience with handling and minimizing Section 702-acquired data, as well as the Section 702 nomination process; during this reporting period, CIA continued to implement this training, which is required for all personnel who nominate facilities to NSA and/or minimize Section 702-acquired communications. FBI has similarly continued implementing its online training programs regarding Section 702 nominations, minimization, and other related requirements. Completion of these FBI online training programs is required of all FBI personnel who request access to Section 702 information. NSD and FBI have also conducted in-person trainings at multiple FBI field offices. For example, during this current reporting period, NSD and FBI continued to provide additional focused training at FBI field offices on the Section

702 minimization procedures, including training FBI field personnel on the attorney-client privileged communication provisions of FBI's minimization procedures.[18] NSD's training at FBI field offices also included training on the reporting requirement from the FISC's *November 6, 2015 Memorandum Opinion and Order* regarding the 2015 FISA Section 702 Certifications. As discussed above, this reporting requirement applies to queries conducted after December 4, 2015, that were conducted solely for the purpose of returning evidence of a crime and returned Section 702-acquired information of or concerning a U.S. person that was reviewed by FBI personnel.

(U) SECTION 3: TRENDS IN SECTION 702 TARGETING AND MINIMIZATION

(U) In conducting the above-described oversight program, NSD, ODNI, and the agencies have collected a substantial amount of data regarding the implementation of Section 702. In this section, a comprehensive collection of this data has been compiled in order to identify overall trends in the agencies' targeting, minimization, and compliance.

(U) I. Trends in NSA Targeting and Minimization

(U) NSA provides to the joint oversight team the average approximate number of facilities that were under collection on any given day during the reporting period. Because the actual number of facilities tasked remains classified,[19] the figure charting the average number of facilities under collection is classified as well. Since the inception of the program, the total number of facilities under collection during each reporting period has steadily increased with the exception of two reporting periods that experienced minor decreases.[20]

[18] (U) This specific training began before and continued after the current reporting period of December 1, 2015 – May 31, 2016.

[19] (U) The provided number of facilities on average subject to acquisition during the reporting period remains classified and is different from the unclassified estimated number of targets affected by Section 702 released by ODNI, most recently in its *2015 Transparency Report*. Previously, ODNI released transparency reports on June 26, 2014, (the *2013 Transparency Report*) and on April 22, 2015 (the *2014 Transparency Report*). The classified numbers estimate the number of *facilities* subject to Section 702 acquisition, whereas the unclassified number provided in the Transparency Reports estimate the number of Section 702 *targets*. As noted in the Transparency Reports, the number of 702 'targets' reflects an estimate of the number of known users of particular facilities subject to intelligence collection under those Certifications. Furthermore, the classified numbers of facilities account for the number of facilities subject to Section 702 acquisition *during the current six month reporting period*, whereas the Transparency Reports estimate the number of targets affected by Section 702 *during the calendar year*.

[20] (U) One of the reporting periods in which the total number of facilities under collection decreased occurred prior to 2010 and is not reflected in the below chart.

Figure 4: ~~(TS//SI//NF)~~ Average Number of Facilities Under Collection



~~(TS//SI//NF)~~ More specifically, NSA reports that, on average, approximately [redacted] facilities were under collection pursuant to the applicable certifications on any given day during the reporting period.[21] This represents an 8.2% increase from the approximately [redacted] facilities under collection on any given day in the last reporting period [redacted]

(U) The above statistics describe the *average* number of facilities under collection at any given time during the reporting period. The total number of *newly* tasked facilities during the reporting period provides another useful metric.[22] Classified Figure 5 charts the total monthly numbers of newly tasked facilities since 2010.

[21] ~~(S//NF)~~ The applicable certifications for this reporting period were [redacted]

[22] (U) The term newly tasked facilities refers to any facility that was added to collection under a certification. This term includes any facility added to collection pursuant to the Section 702 targeting procedures; some of these newly tasked facilities are therefore facilities that had been previously tasked for collection, were detasked, and now have been retasked.

Figure 5: ~~(TS//SI//NF)~~ New Taskings by Month (Yearly Average for 2010 through Nov. 2015)



~~(S//SI//NF)~~ Specifically, NSA provided documentation of [redacted] new taskings during the reporting period. This represents a 25.7% increase in new taskings from the previous reporting period. [redacted]

~~(S//SI//NF)~~ During the first eleven months of 2015, NSA has tasked an average of [redacted] telephony facilities. During this reporting period, NSA tasked an average of [redacted] telephony facilities per month. This represents a [redacted] increase in the average monthly telephony facilities in this reporting period compared to the first eleven months of 2015.

~~(S//SI//NF)~~ NSA tasked an average of [redacted] electronic communications accounts during the first eleven months of 2015. During this reporting period, NSA tasked an average of [redacted] electronic communication accounts (a [redacted] increase from the 2015 monthly average through November).

(U) With respect to minimization, NSA identified to the joint oversight team the number of serialized reports NSA generated based upon minimized Section 702-acquired data, and provided NSD and ODNI access to all reports NSA identified as containing United States person

information.[23] Figure 6 contains the classified number of serialized reports and reports identified as containing United States person information over the last ten reporting periods. NSD and ODNI's review revealed that the United States person information was at least initially masked in the vast majority of circumstances.[24] The number of serialized reports NSA has identified as containing United States person information slightly decreased for the second consecutive reporting period.

Figure 6: ~~(S//NF)~~ Total Disseminated NSA Serialized Reports Based Upon Section 702-Acquired Data and Number of Such Reports NSA Identified as Containing USP Information



~~(S//NF)~~ Specifically, in this reporting period NSA identified to NSD and ODNI [redacted] serialized reports based upon minimized Section 702-acquired data. This represents a 3.0%

[23] (U) Previous joint assessments referred to these reports containing minimized Section 702- or Protect America Act (PAA)-acquired information. However, given that Section 702 of FAA replaced the PAA in 2008, the government no longer disseminates minimized information that was previously acquired pursuant to PAA. However, Figure 6 provides a trend analysis over a longer period of time and may include reports containing minimized PAA-acquired information in addition to minimized Section 702-acquired information.

[24] (U) NSA generally "masks" United States person information by replacing the name or other identifying information of the United States person with a generic term, such as "United States person #1." Agencies may request that NSA "unmask" the United States person identity. Prior to such unmasking, NSA must determine that disseminating the United States person's identity meets one of the specified reasons listed in NSA's minimization procedures, including that the U.S. person consented to the dissemination, the U.S. person information was already publicly available, the U.S. person identity was necessary to understand foreign intelligence information, or the communication contained evidence of a crime and is being disseminated to law enforcement authorities. Even if one these conditions applies, as a matter of policy, NSA may still mask the U.S. person information and will include no more than the minimum amount of U.S. person information necessary to understand the foreign intelligence or to describe the crime or threat.

increase from the [redacted] such serialized reports NSA identified in the prior reporting period. Figure 6 reflects NSA reporting over the last ten reporting periods; the fact that reporting based on Section 702 -acquired data increased is consistent with prior reporting periods.

~~(S//NF)~~ Figure 6 also shows the number of these serialized reports that NSA identified as containing United States person information. During this reporting period, NSA identified [redacted] serialized reports as containing United States person information derived from Section 702-acquired data.[25] The percentage of reports containing United States person information was lower this reporting period (8.5 %), than the 9.0% and 9.7% reported in the two prior reporting periods.

(U) II. Trends in FBI Targeting

(U) Under Section 702, NSA designates and submits facilities to FBI for acquisition of communications from certain facilities that have been previously approved for Section 702 acquisition under the NSA targeting procedures. FBI applies its own targeting procedures with regard to these designated accounts. FBI reports to the joint oversight team the specific number of facilities designated by NSA and the number of NSA designated-facilities that FBI approved.[26] As detailed below, the number of facilities designated for acquisition has increased from the past reporting period, which is consistent with the general trend in prior reporting periods.[27]

(U) As classified Figure 7 details, FBI approves the vast majority of NSA's designated facilities and this percentage has been consistently high. The high level of approval can be attributed to the fact that the NSA-designated facilities have already been evaluated and found to meet NSA's targeting procedures. FBI may not approve NSA's request for acquisition of a designated facility for several reasons, including withdrawal of the request because the potential data to be acquired is no longer of foreign intelligence interest, or because FBI has uncovered information causing NSA and/or FBI to question whether the user or users of the facility are non-United States persons located outside the United States. Historically, the joint oversight team notes that for those accounts not approved by FBI, only a small portion[28] were rejected on the basis that they were ineligible for Section 702 collection.

[25] (U) NSA does not maintain records that allow it to readily determine, in the case of a report that includes information from several sources, from which source a reference to a U.S. person was derived. Accordingly, the references to U.S. person identities may have resulted from collection pursuant to Section 702 or from other authorized signals intelligence activity conducted by NSA that was reported in conjunction with information acquired under Section 702. Thus, the number provided above is assessed to likely be over-inclusive. NSA has previously provided this explanation in its Annual Review pursuant to Section 702(l)(3) that is provided to Congress.

[26] [redacted]

[27] [redacted]

[28] [redacted]

(U) Between 2010 and December 2013, the *yearly average* of designated facilities approved by FBI steadily increased. The average of designated facilities approved by the FBI in 2014 slightly decreased. Between January and November 2015, the *number* of designated facilities approved by FBI *each month* has varied. NSD and ODNI have continued to track the number of facilities approved by FBI in 2015 and will incorporate this information into future Joint Assessments.

Figure 7: [redacted]

~~(S//SI//NF)~~ Specifically, FBI reports that NSA designated [redacted] accounts [redacted] during the reporting period – an average of [redacted] designated accounts per month. This is a [redacted] increase from the [redacted] accounts designated in the prior six-month reporting period. [redacted]

~~(S//NF)~~ FBI approved [redacted][29] requests [redacted]

(U) As indicated in prior Joint Assessments, the Government was previously able to provide figures regarding the number of reports FBI had identified as containing minimized Section 702-acquired United States person information. However, in 2013, FBI transitioned much of its dissemination of Section 702-acquired information from FBI Headquarters to FBI field offices. NSD conducts oversight reviews at multiple FBI field offices each year, some of which ODNI attends, and during those reviews, NSD reviews a sample of the Section 702 disseminations issued by the respective field office. Because every field office is not reviewed every six months, NSD no longer has comprehensive numbers on the number of disseminations of Section 702-acquired United States person information made by FBI. FBI does, however, report comparable information on an annual basis to Congress and the FISC pursuant to 50 U.S.C. § 1881a(l)(3)(i).

(U) III. Trends in CIA Minimization

(U) CIA only identifies for NSD and ODNI disseminations of Section 702-acquired United States person information. Classified Figure 8 compiles the number of such disseminations of reports containing United States person information identified in the last ten reporting periods (June-November 2011 through the current period of December 2015 - May 2016). In the first six reporting periods, the number of CIA-identified disseminations containing United States person information, while always low, decreased. In the seventh, the number of CIA-identified disseminations containing United States person information, while still low, increased. In the prior two reporting periods, the number of CIA-identified disseminations containing United States person information again decreased. In this reporting period, the number of CIA-identified disseminations containing United States person information increased.

[29] ~~(S//NF)~~ The Government previously reported that the FBI approved approximately [redacted]

Figure 8: ~~(S//NF)~~ Disseminations Identified by CIA as Containing Minimized Section 702-Acquired United States Person Information (Excluding Certain Disseminations to NCTC)

[redacted]

~~(S//NF)~~ During this reporting period, CIA identified [redacted] disseminations of Section 702-acquired data containing minimized United States person information. This is a [redacted] increase from the [redacted] such disseminations CIA made in the prior reporting period and is the highest number of such disseminations since the June 2012 through November 2012 reporting period. [redacted] and as reported in prior Joint Assessments, CIA also permits some personnel with [redacted] NSD and ODNI, however, review all [redacted] containing Section 702-acquired information that CIA has identified as potentially containing United States person information to ensure compliance with CIA's minimization procedures.

(U) CIA also tracks the number of files its personnel determine are appropriate for broader access and longer-term retention. CIA's minimization procedures must be applied to these files before they are retained or transferred to systems with broader access.[30] Classified Figure 9 details

[30] ~~(S//NF)~~ [redacted] n making these retention decisions, CIA personnel are required to identify any files potentially containing United States person information.

the total number of files that were either retained or transferred, as well as the number of those retained or transferred files that contain identified United States person information.[31] Beginning in the middle of the reporting period covered by the thirteenth Joint Assessment (dated September 2015), CIA began reporting the number of files CIA transferred to systems with broader access, instead of the number of files retained in systems of limited access, as the number of transferred files provides a more accurate portrayal of CIA's use of Section 702-acquired information. This current assessment reports the total number of files CIA transferred from December 2015 through May 2016. For reference, however, the number of files retained from prior assessment periods is also displayed in the Figure below.[32] In all reporting periods, the number of retained or transferred files identified by CIA as potentially containing United States person information has been consistently a very small percentage of the total number of retained or transferred files.

[31] (U) As reported in the eleventh Joint Assessment (October 2014), CIA determined in September 2014 that characterizations in prior assessments of the number of files having been "transferred" was not the most appropriate term as some files had been retained for long term retention but had not been transferred to systems of broader access. Consequently, the numbers of files for which CIA had made a retention decision were re-characterized as having been "retained." Because the terms transferred and retained attempt to describe the same authorized actions under CIA's Minimization Procedures, this Joint Assessment just refers to retention decisions.

[32] [redacted]

Figure 9: ~~(S//NF)~~ Total CIA Files Retained or Transferred and Total CIA Files that were Retained or Transferred Files Which Contained Potential United States Person Information



~~(S//NF)~~ For this reporting period, CIA analysts transferred or retained [redacted] of which were identified by CIA as containing a communication with potential United States person information. This is a [redacted] decrease in the number of files transferred or retained, when compared to the previous reporting period when [redacted] of which contained potential United States person information.

(U) SECTION 4: COMPLIANCE ASSESSMENT – FINDINGS

(U) The joint oversight team finds that during this reporting period, the agencies have continued to implement the procedures and follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702. The personnel involved in implementing the authorities are appropriately directing their efforts at non-United States persons reasonably believed to be located outside the United States for the purpose of acquiring foreign intelligence information. Processes have been put in place to implement these authorities and to impose internal controls for compliance and verification purposes.

(U) The compliance incidents during the reporting period represent a very small percentage of the overall collection activity. Based upon a review of the reported compliance incidents, the joint oversight team does not believe that these incidents represent an intentional attempt to circumvent or violate the procedures required by the Act.

(U) As noted in prior reports, in the cooperative environment the implementing agencies have established, an action by one agency can result in an incident of noncompliance with another agency's procedures. It is also important to note that a single incident can have broader implications.

(U) Each of the compliance incidents for this current reporting period are described in detail in the corresponding Section 707 Report. The Joint Assessment provides NSD and ODNI's analysis of those compliance incidents in an effort to identify existing patterns or trends that might identify the underlying causes of those incidents. The joint oversight team then considers whether and how those underlying causes could be addressed through additional remedial or proactive measures and assesses whether the agency involved has implemented appropriate procedures to prevent recurrences. The joint oversight team continues to assist in the development of such measures, some of which are detailed below, especially as it pertains to investigating whether additional and/or new system automation may assist in preventing compliance incidents.

(U) I. Compliance Incidents – General

(U) A. Statistical Data Relating To Compliance Incidents

~~(S//NF)~~ As noted in the Section 707 Report, there were a total of [redacted][33] compliance incidents that involved noncompliance with NSA's targeting or minimization procedures and [redacted] compliance incidents involving noncompliance with FBI's targeting and minimization procedures,

[33] ~~(S//NF)~~ The Government mistakenly reported the total number of compliance incidents as [redacted] during this reporting period in the September 2016 *Semiannual Report of the Attorney General Concerning Acquisitions Under Section 702 of the Foreign Intelligence Surveillance Act* (i.e. the Section 707 Report). One detasking delay was inadvertently not counted. Thus, the correct number of compliance incidents involving NSA's targeting or minimization procedures is [redacted]

for a total of [redacted] incidents involving NSA and/or FBI procedures.[34] During this reporting period, there were no identified incidents of noncompliance with CIA's minimization procedures. There were [redacted] identified instances of noncompliance by an electronic communication service provider issued a directive pursuant to Section 702(h) of FISA.

(U) The following table puts these compliance incidents in the context of the average number of facilities subject to acquisition on any given day[35] during the reporting period:

Figure 10: ~~(TS//SI//NF)~~ Compliance Incident Rate

Compliance incidents during reporting period (December 1, 2015 – May 31, 2016)	[redacted]
Number of facilities on average subject to acquisition during the reporting period	[redacted]
Compliance incident rate: number of incidents divided by average facilities subject to acquisition	0.45%

(U) The compliance incident rate continues to remain low, with the current rate of 0.45% representing a decrease from the 0.53% compliance incident rate in the prior reporting period.[36] The number of notification delays remained low during this reporting period. If the notification delays incidents are not included in the calculation, the overall compliance incident rate for this reporting period is actually 0.42%. This information is explained below and detailed in Figure 11.

(U) While the incident rate remains low, this percentage in and of itself does not provide a full measure of compliance in the program. A single incident, for example, may have broad ramifications and may involve multiple facilities. Other incidents, such as notification delays

[34] (U) As is discussed in the Section 707 report and herein, some compliance incidents involve more than one element of the Intelligence Community. Incidents have therefore been grouped not by the agency "at fault," but instead by the set of procedures with which actions have been noncompliant.

[35] ~~(S//NF)~~ [redacted] he Attorney General's Section 707 report provides further details with respect to any particular incident.

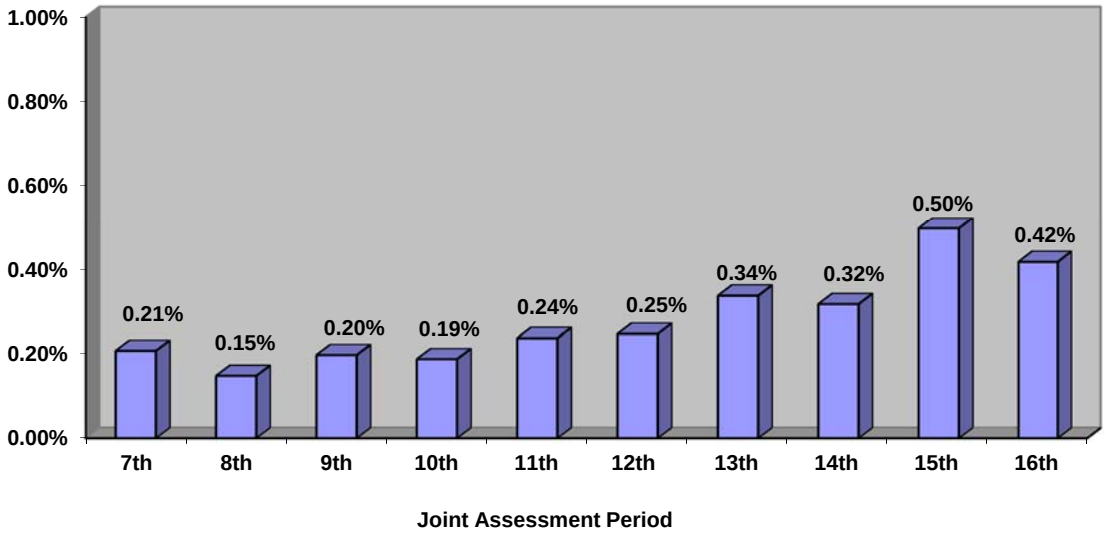
[redacted]

[36] ~~(TS//SI//NF)~~ As explained in the prior Joint Assessment, the Government assessed the 0.53% figure to be largely attributable to two types of errors. For example, [redacted] of these previously reported incidents of noncompliance with NSA's procedures [redacted]

(described further below) may occur with frequency, but have limited significance with respect to United States person information.[37]

(U) The joint oversight team assesses that another measure of substantive compliance with the applicable targeting and minimization procedures is to compare the compliance incident rate excluding these notification delays. The following Figure 11 shows this adjusted rate:

Figure 11: (U) Compliance Incident Rate (as the number of incidents divided by the number of average facilities tasked), Not including Notification Delays



(U) As Figure 11 demonstrates, the adjusted compliance incident rate calculated without the notification delays is 0.42%, which is lower than what was reported in the prior reporting period (0.50%) and still well below 1%. The joint oversight team assesses that the consistently low compliance incident rate of less than 1% is a result of training, internal processes designed to identify and remediate potential compliance issues, and a continued focus by internal and external oversight personnel to ensure compliance with the applicable targeting and minimization procedures.

[37] (U) The Joint Assessment has traditionally compared the number of compliance incidents to the number of average tasked facilities. Using the number of average facilities subject to acquisition as the denominator provides a general proxy for an activity level that is relevant from a compliance perspective. That is, the joint oversight team believes that the number of targeted facilities generally comports with the number of activities that could result in compliance incidents (*e.g.* taskings, detaskings, disseminations, and queries). Tracking this rate over consecutive years allows one to discern general trends as to how the Section 702 program is functioning overall from a compliance standpoint.

(U) B. Categories of Compliance Incidents

(U) Most of the compliance incidents occurring during the reporting period involved non-compliance with the NSA's targeting or minimization procedures. This largely reflects the centrality of NSA's targeting and minimization efforts in the Government's implementation of the Section 702 authority. The compliance incidents involving NSA's targeting or minimization procedures have generally fallen into the following categories:

- (U) *Tasking Issues.* This category involves incidents where noncompliance with the targeting procedures resulted in an error in the initial tasking of the facility.

- (U) *Detasking Issues.* This category involves incidents in which the facility was properly tasked in accordance with the targeting procedures, but errors in the detasking of the facility caused noncompliance with the targeting procedures.

- (U) *Notification Delays*. This category involves incidents in which a facility was properly tasked in accordance with the targeting procedures, but a notification requirement contained in the targeting procedures was not satisfied.

- (U) *Documentation Issues.* This category involves incidents where the determination to target a facility was not properly documented as required by the targeting procedures.[38]

- (U) *Minimization Issues.* This category involves NSA's compliance with its minimization procedures.

- (U) *Other Issues.* This category involves incidents that do not fall into one of the six above categories.

In some instances, an incident may involve more than one category of noncompliance.

(U) These categories are helpful for purposes of reporting and understanding the compliance incidents. Because the actual number of incidents remains classified, Figure 12A depicts the percentage of compliance incidents in each category that occurred during this reporting period, whereas Figure 12B provides that actual classified number of incidents.

[38] (U) As described in the Section 707 Report, not all documentation errors are separately enumerated as compliance incidents.

Figure 12A: (U) Percentage Breakdown of Compliance Incidents Involving the NSA Targeting and Minimization Procedures

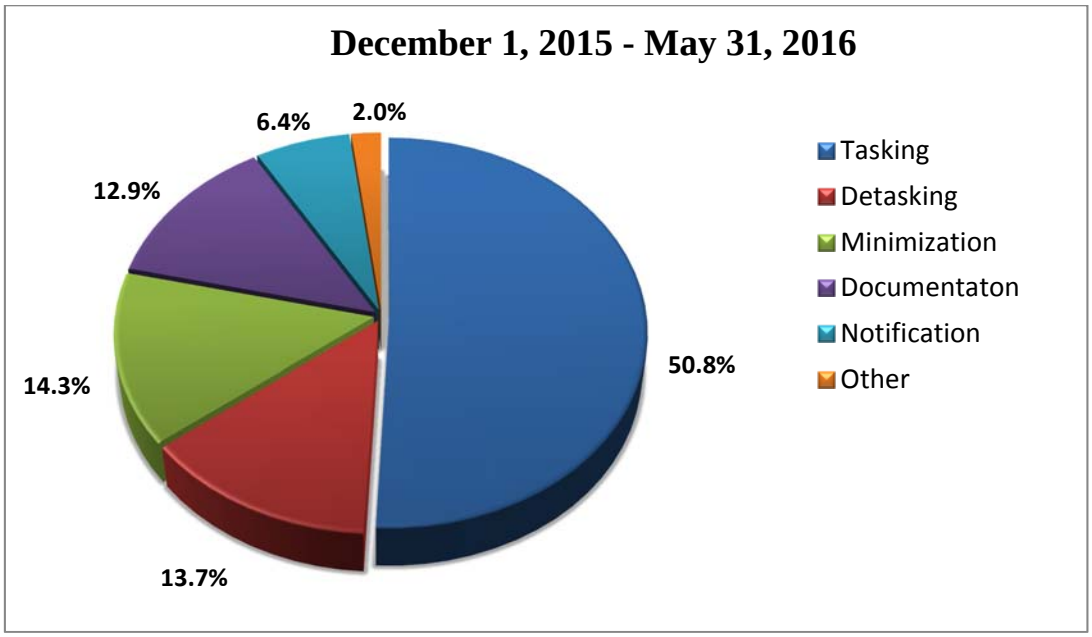


Figure 12B: ~~(S//NF)~~ Number of Compliance Incidents Involving the NSA Targeting and Minimization Procedures

[redacted]

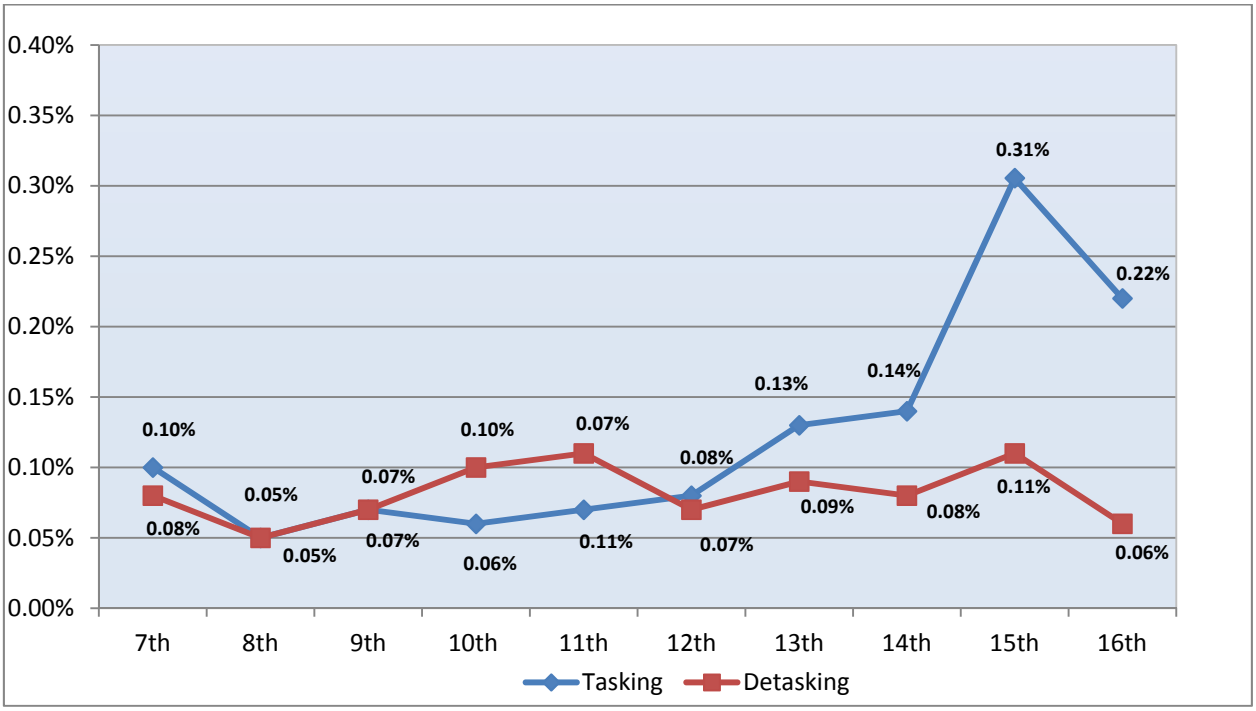
(U) As Figures 12A and B demonstrate, the proportion of notification delays, which used to constitute the predominant share of incidents, remains low. Tasking and detasking incidents often involve more substantive compliance incidents insofar as they can (but do not always) involve collection involving a facility used by a United States person or an individual located in the United States. Furthermore, incidents of noncompliance with minimization procedures are also a focus of the joint oversight team because these types of incidents may involve information concerning United States persons.

~~(S//NF)~~ More specifically, the number of tasking incidents decreased [redacted]; detasking incidents decreased [redacted]; minimization incidents increased [redacted]; documentation incidents increased [redacted];[39] and "other" category incidents decreased [redacted]. The number of notification delays increased slightly [redacted]. There were zero overcollection incidents in this period, which is consistent with the zero overcollection incidents reported for the prior period.

(U) The following chart, Figure 13, depicts the compliance incident rates, as compared to the average facilities on task, for tasking and detasking incidents over the previous reporting periods. While these tasking and detasking incidents are grouped in a single chart for a comparison, the tasking and detasking incidents are not relational to each other, *i.e.* an increase or decrease in the rate of tasking incidents does not result in an increase or decrease in the detasking incident rate.

[39] ~~(S//NF)~~ The tracking of documentation errors above reveals an increase in the number of documentation errors between the last reporting period and the current reporting period. The joint oversight team assesses that this increase is partly attributable to a previous change in NSA's targeting procedures. As explained in the last joint assessment (i.e., the 15th Joint Assessment dated November 2016), NSA's targeting procedures approved by the FISC in November 2015 included a then-new documentation requirement that NSA provide a written explanation of the basis for the assessment, at the time of targeting, that the target possesses, is expected to receive, and/or is likely to communicate foreign intelligence information concerning the foreign power or foreign territory that is covered by the certification under which the accounts were tasked. Under prior Section 702 targeting procedures, although analysts were required under the targeting procedures to conduct an analysis regarding why the targeting of the user of a facility would result in obtaining foreign intelligence information under the Section 702 certifications, analysts were not required to document this foreign intelligence purpose determination in the same manner as they were required to document the foreignness determination. In addition, by policy, NSA previously required all taskings to be accompanied by a brief statement explaining the analyst's rationale for assessing that the tasking of the facility would result in the acquisition of the types of foreign intelligence information authorized by the Section 702 certifications. The Privacy and Civil Liberties Oversight Board (PCLOB), in its July 2014 Section 702 Report, recommended that the targeting procedures be updated to include a requirement that each tasking include a written explanation of the foreign intelligence purpose of each targeting decision. After the FISC approved NSA's 2015 targeting procedures with the then-new documentation requirement, any non-compliance with this requirement was counted as a documentation error and reported to the applicable oversight entities. With the then-new documentation requirement, the joint oversight team began examining whether the team should revise the counting of documentation errors to address NSA's revised targeting procedures. Thus, while the joint oversight team assesses that the increase in documentation errors partially resulted from NSA analysts failing to properly document the new written justification requirement, the team also assessed that a change in the government's methodology for counting documentation errors contributed to a small increase in the amount of documentation errors. As it pertains to the Government's counting methodology, historically, in calculating the total number of documentation errors, the Government only included incidents, in which the documentation indicated that NSA intended to task a facility to a different DNI/AG Section 702(g) certification than the certification under which the facility was actually tasked. The revised methodology includes failure to comply with the requirement that NSA's documentation concerning each tasked facility contain a citation to the source of information upon which the determination that the user of that facility was reasonably believed to be located outside the United States was made (the "foreignness determination"); these type of documentation errors were not previously counted in this category.

Figure 13: (U) Tasking and Detasking Incident Compliance Rates



(U) Over the time periods covered in the above chart, the tasking and detasking incident compliance rate has varied by fractions of a percentage point as compared to the average size of the collection. Tasking errors cover a variety of incidents, ranging from the tasking of an account that the Government should have known was used by a United States person or an individual located in the United States to typographical errors in the initial tasking of the account that affect no United States persons or persons located in the United States.[40] On the other hand, detasking errors more often involve a facility used by a United States person or an individual located in the United States, who may or may not have been the targeted user.[41] The percentage of compliance incidents involving such detasking incidents has remained consistently low.[42]

[40] (U) As discussed in detail in the previous joint assessment, the significant increase in tasking errors during the 15th joint assessment reporting period was substantially caused by one particular NSA targeting office misunderstanding the requirements of the targeting procedures. As a result, that particular targeting office was required to retake NSA's formal Section 702 online training. *See* the 15th Joint Assessment, pp. 35 – 36.

[41] [redacted]

[42] (U) NSD and ODNI note that the above incident rates fluctuate by hundredths of a percentage point. Any perceived significant fluctuation is due to the scale of the graph (.00% to .25%). If, for example, the chart used a 0% to 1% scale to show fluctuations, the chart would show two virtually flat lines hugging the bottom. NSD and ODNI do not believe that any of the different incident rates are statistically significant, and note that the incident rate is consistently quite low.

(U) With respect to FBI's targeting and minimization procedures, incidents of non-compliance with the FBI targeting procedures increased from a rate below 0.01% in the prior reporting period to 0.01% in the current reporting period.[43] The total number of identified minimization errors also remains low.[44] The joint oversight team assesses that FBI's overall compliance with its targeting and minimization procedures is a result of FBI's training and the processes it has designed to effectuate its procedures.

(U) Furthermore, there are no incidents during this reporting period that involved CIA's minimization procedures, which is less than the one incident that occurred during the previous reporting period for CIA. The joint oversight team assesses that CIA's compliance is a result of its training, systems and processes that were implemented when the Section 702 program was developed to ensure compliance with its minimization procedures, and the work of its internal oversight team.

~~(S//NF)~~ Finally, there were [redacted] incidents of non-compliance caused by errors made by a communications service provider in this reporting period, which represents an increase from the zero incidents reported in the prior reporting period. The joint oversight team assesses that the low number of errors by the communications service providers is the result of continuous efforts by the Government and providers to ensure that lawful intercept systems effectively comply with the law while protecting the privacy of the providers' customers.

(U) II. Review of Compliance Incidents – NSA Targeting and Minimization Procedures

(U) As with the prior Joint Assessment, this Joint Assessment takes a broad approach and discusses the trends, patterns, and underlying causes of the compliance incidents reported in the Section 707 Report. The joint oversight team believes that analyzing the trends of these incidents, especially in regard to their causes, helps the agencies focus resources, avoid future incidents, and improve overall compliance. The Joint Assessment primarily focuses on incidents involving NSA's targeting and minimization procedures, the volume and nature of which are better-suited to detecting such patterns and trends. The following subsections examine incidents of non-compliance involving NSA's targeting and minimization procedures. Most of these incidents did not involve United States persons, and instead involved matters such as typographical or other tasking errors, detasking delays with respect to facilities used by non-United States persons who may have entered the United States, or notification delays. Some incidents during this reporting period did, however, involve United States persons. United States persons were primarily impacted by: (1) tasking errors that led to the tasking of facilities used by United States persons; (2) delays in detasking facilities after NSA determined that the user of the facility was a United States person; and (3) non-compliance with the NSA's minimization procedures involving the unintentional improper dissemination, retention, or querying of Section 702 information.

[redacted]

43 [redacted]

44 [redacted]

(U) In the subsections that follow,[45] this Joint Assessment examines some of the underlying causes of incidents of non-compliance that contributed to the compliance incident rate of 0.45%. This Joint Assessment focuses on examining and explaining incidents that have the greatest potential to impact United States persons' privacy interests, even though those incidents represent a minority of the overall incidents.

(U) A. Reverse Targeting

(U) One of NSA's tasking errors[46] involved the tasking of a facility that was used by a non-United States person located outside the United States that was determined to involve reverse targeting. Reverse targeting occurs when NSA tasks a communication facility used by a non-United States person reasonably located outside the United States for the purpose of acquiring the communications of a United States person or a person located in the United States. Reverse targeting is barred by statute and NSA policy and the prevention of reverse targeting is a key component of both the internal and external review of the Section 702 program.[47]

(U) This incident involved a United States person whom the FISC had found probable cause to believe was an agent of a foreign power pursuant to Title I of FISA and whom the Attorney General had authorized the targeting of pursuant to Section 705(b) of FISA. This reverse targeting incident resulted from an NSA analyst misunderstanding the reverse targeting prohibition and not because an NSA analyst intentionally attempted to violate Section 702 or NSA policy.[48] Despite the misunderstanding of law that caused this current incident, the joint oversight team assesses that the extreme rarity of reverse targeting incidents demonstrates the success of NSA's training efforts on this issue.

---

[45] (U) While ODNI and DOJ strive to maintain consistency in the headings of these subsections, these headings may nonetheless change with each joint assessment depending on the incidents that occurred in each reporting period and their respective underlying causes.

[46] [redacted]

[47] (U) Among other things, Section 702 requires the Attorney General, in consultation with the DNI, to adopt guidelines to ensure compliance with Section 702's targeting restrictions. The Attorney General's guidelines state, "Intelligence agencies may not designate a nominal non-U.S. person foreign target when the actual target is a U.S. communicant with whom that foreign target is known to be in contact." In other words, the guidelines prohibit reverse targeting of either persons located inside the United States, regardless of their nationality, or United States persons, regardless of their location.

[48] [redacted]

(U) B. Due Diligence and Pre-Tasking Information

(U) During this reporting period, a number of incidents involved the failure to conduct necessary foreignness checks or to otherwise exercise due diligence prior to the tasking of a facility. Approximately 37% of the tasking errors in this reporting period involved instances in which NSA did not take sufficient pre-tasking steps to try to find information regarding the location of the targeted user or otherwise did not properly establish a sufficient basis to assess that the targeted user was outside the United States. The two most common examples include situations in which the analyst did not conduct a necessary pre-tasking check or there was too long of a delay between the necessary pre-tasking checks and the actual tasking of the account.[49] To address these types of tasking errors, NSA has sent out multiple reminders or compliance advisories to its analysts and tasking adjudicators, reminding them of the pre-tasking requirements. These reminders have also been posted on NSA's internal websites for personnel who handle Section 702 collection. Furthermore, NSA intends to update its Section 702 training to emphasize the issues contributing to these tasking errors.

~~(TS//SI//NF)~~ One example of NSA failing to conduct sufficient pre-tasking foreignness checks occurred with respect to the tasking [redacted] NSA detasked the facilities and advised that there was no indication that the facilities were used by a United States person or by someone in the United States. [redacted]

[49] [redacted]

[redacted]

(U) D. Effect of Other Technical Issues

(U) There were a small number of compliance incidents resulting from technical issues during this reporting period. Technical issues potentially have larger implications than other incidents because technical issues: often involve more than one facility; can remain undetected and uncorrected for a long period of time; and can proliferate dramatically in a short time period, including across numerous interconnected systems. As such, all agencies involved in the Section 702 program devote substantial resources towards the prevention, identification, and remedy of technical issues. Collection equipment and other related systems undergo substantial testing prior to deployment. The agencies also employ a variety of monitoring programs to detect anomalies in order to prevent or limit the effect of technical issues on acquisition. Members of the joint oversight team participate in technical briefings at the various agencies to better understand how technical system development and modifications affect the collection and processing of information. As a result of these efforts, potential issues have been identified, the resolution of which prevented compliance incidents from happening and ensured the continued flow of foreign intelligence information to the agencies. The joint oversight team believes that the historically limited number of overcollection incidents is the result of the efforts of all of the involved agencies.

50 [redacted]

51 [redacted]

While technical issues can potentially have larger implications, this potential was largely avoided during this reporting period.

(U) Specifically, the technical issues that resulted in delayed detaskings were caused by system errors and data not being properly processed due to a server backlog.[52] In these instances, the technology and systems failed to function as designed, and, thus, the systems failed. This resulted in delayed detasking incidents, whereby NSA was unable to timely detask facilities. NSA subsequently corrected these technical issues. Additionally, none of the users of the facilities at issue were believed to be United States persons.

~~(S//NF)~~ There were [redacted] incidents related to NSA's [redacted] post-tasking [redacted] the required post-tasking checks were rerun to ensure that any use of a Section 702-tasked facility from within the United States was identified and, if so identified, the requisite purges were conducted.

(U) E. Effect of Human Errors

(U) As reported in previous Joint Assessments, human errors caused some of the identified compliance incidents. Each of the agencies has established a variety of processes to both reduce human errors and to identify such errors when they occur. These processes have helped to limit such errors, but some categories of human errors are unlikely to be entirely eliminated. For example, despite multiple pre-tasking checks, instances of typographical errors or similar errors occurred in the targeting process that caused NSA to enter the wrong facility into the collection system. Such typographical errors accounted for approximately 18% of the tasking errors made in this reporting period, which is an increase from the previous reporting period, in which typographical errors accounted for 4% of the tasking errors.[55] Approximately 22% of the detasking

52 [redacted]

53 [redacted]

54 [redacted]

55 [redacted]

delays[56] from this reporting period were the result of inadvertent errors, such as an NSA analyst detasking some, but not all, of a target's facilities that required detasking.[57] In addition, approximately 13% of the detasking delays were the result of faulty analysis or misunderstanding of the targeting procedures.[58] As with other compliance incidents, any data acquired as a result of such tasking and detasking errors - regardless of whether or not the user proves to be a United States person or person in the United States - is required to be purged.

(U) While the joint oversight team assesses that existing practices and systems adequately reduce the number of incidents discussed above, the joint oversight team assesses that other errors could potentially be reduced with new training, procedures or system modifications. The following subdivides such incidents into errors that could be addressed through system or process changes and those that could be potentially reduced through training. Independent of the broader system, process, or training changes suggested below, in each of the individual incidents discussed below, data acquired as a result of the specific incidents has been purged and the personnel directly involved have been reinstructed regarding the applicable requirements.

(U) (1) Minimization Errors That Can Be Addressed Through Training and Technical Improvements

(U) NSA's minimization procedures include several restrictions on querying raw Section 702 collection. First, queries of raw Section 702 collection must be designed in a manner "reasonably likely to return foreign intelligence information" to prevent overly broad queries. In addition, although NSA's Section 702 minimization procedures permit queries of raw Section 702 collection using United States person identifiers, such queries are to first be approved in accordance with NSA's internal procedures. And, NSA's Section 702 minimization procedures, in effect during this reporting period, prohibited using United States person identifiers to query Internet communications acquired through NSA's upstream collection techniques. During this reporting period, approximately 86% of the minimization procedure errors involved non-compliance with NSA's minimization rules regarding queries (whereas it was approximately 56% in the previous reporting period).[59] As with prior Joint Assessments, query incidents remain the cause of most compliance incidents involving NSA's minimization procedures.

[56] ~~(U//FOUO)~~ This percentage is slightly higher than the percentage of these types of detasking delays reported in the prior Joint Assessment.

[57] [redacted]

[58] [redacted]

[59] [redacted]

(U) Specifically, during this reporting period, 44% of the query incidents involved overly broad queries.[60] These overly broad query errors are typically traceable to a typographical or comparable error in the construction for the query. For example, an overly broad query can be caused when an analyst mistakenly inserts an "or" instead of an "and" in constructing a Boolean query, and thereby potentially received overly broad results as a result of the query. As with previous reporting periods, there were no incidents of an analyst purposely running a query for non-foreign intelligence purposes against Section 702-acquired data identified during the reporting period.

(U) The remaining query incidents involved NSA analysts: (a) using United States person identifiers which had not been approved pursuant to NSA's internal procedures to query Section 702-acquired data; (b) exceeding the scope of the authorization provided under NSA's internal procedures; and/or (c) using approved United States person identifiers to query Internet communications acquired through NSA's upstream collection techniques.

(U) During the reporting period, the joint oversight team identified a substantial increase in the number of minimization incidents involving United States person queries, primarily attributable to upstream query incidents. Through additional discussions with NSA after the current reporting period, the joint oversight team learned of additional improper queries discovered by NSA's Office of Compliance Operations (OCO) and Office of the Inspector General (OIG) involving United States person identifiers queried in Section 702 upstream collection. Some of the improper queries identified in studies conducted by OCO and the OIG were conducted during this reporting period. While additional discussions and notices to the Court occurred outside this Joint Assessment's reporting, the most up-to-date information is being provided here to give as complete of a description of the incidents as possible.

~~(S//SI//NF)~~ As background, some of the improper upstream queries were initially identified by NSA's OIG in a study that culminated in a report issued in January 2016.[61] As part of this study, the OIG reviewed queries conducted between January and March 2015 that included United States person identifiers associated with Section 704 or 705(b) targets. The January 2016 OIG's report noted that NSA's former Signals Intelligence Directorate (SID) Oversight and Compliance (O&C) section[62] opined that the upstream queries were conducted because [redacted] all authorities to which analysts were entitled access on the basis of their credentials.[63] NSA's O&C opined that analysts had not removed the Section 702 upstream authority from their query criteria or had not included other appropriate limiters to prevent Section 702 upstream data from being queried.

[60] [redacted]

[61] (U) NSA's January 7, 2016 Inspector General Report was publicly released on *IC on the Record* on May 11, 2017.

[62] (U) NSA's SID O&C section was replaced by NSA OCO on August 31, 2016, as part of NSA internal reorganization.

[63] ~~(U//FOUO)~~ NSA now knows that [redacted] issue occurred not only in legacy systems, but in NSA's modernized systems, as well.

~~(S//SI//NF)~~ NSA then initiated additional compliance verification studies of queries of upstream data to address the OIG's findings. [redacted] NSA determined that human error was the primary factor in all of the improper queries identified even though the analysts were knowledgeable of the prohibition against querying United States person identifiers in Section 702 upstream data.[64] Specifically, the majority of the improper queries were caused when an analyst failed to de-select Section 702 upstream data from the list of authorities even though the analyst knew that he or she was conducting a query using a United States person identifier. For some of the other improper queries, the analysts conducted reasonable due diligence to determine whether their queries included one or more United States person identifiers and evidence of United States person status was returned by NSA's systems, but, due to the amount or complexity of information presented by some of NSA's systems, the analysts overlooked the evidence of United States person status and failed to limit the subsequent query accordingly. The remaining identified improper upstream queries resulted from a lack of due diligence by analysts. Before conducting any query, NSA analysts are trained to take certain steps to determine whether an identifier to be queried is associated with a United States person. For these queries, the analysts failed to take all of the necessary steps before conducting the query.

(U) On October 26, 2016, the Government submitted a written notice regarding these improper queries – using U.S. person identifiers to query Section 702 upstream collection – and the status of NSA's investigation into these queries. That same day, the FISC held a hearing on this matter. As a result of these compliance issues and timing of the notification, the FISC extended the statutorily-prescribed time limits for the Court to complete its review of the 2016 Certifications and ordered that the time limit be extended through January 31, 2017. On January 27, 2017, the government sought an additional extension of time to address the upstream query issue. That same day, the FISC issued an Order, extending the time limit for the Court to complete its review of the 2016 Certifications to April 28, 2017.[65] Although the government continues to investigate these issues, NSA has taken significant steps to limit the instances of non-compliant queries of upstream Section 702 data.

~~(TS//SI//NF)~~ NSA conducted another study (between November and December 2016) to further understand the scope of the issue. In this study, NSA reviewed known United States person

[64] ~~(U//FOUO)~~ Only one analyst was unaware of the prohibition. This analyst received the Section 702 training, but did not take away from the training the rule that United States person identifiers cannot be queried in Section 702 upstream data. This analyst has since received additional guidance.

[65] (U) While outside this current joint assessment's reporting period, this assessment notes that during the FISC ordered extension periods, NSA undertook a broad review of its Section 702 program and subsequently determined that it would no longer collect communications "about" a target. See ODNI's *IC on the Record* public statement dated May 11, 2017, concerning the *Release of FISC Opinion Approving the 2016 Section 702 Certifications and Other Related Documents*. After the Government reported NSA's remedial steps to the FISC, the FISC issued its *Memorandum and Opinion* on April 26, 2017, approving the 2016 Section 702 Certifications, because, in part as it pertains to the above-described incident, the FISC determined that the changes NSA made to its upstream Internet collection sufficiently addressed the compliance incidents involving the inadvertent use of U.S. person identifiers as query terms. See the FISC's April 2017 Opinion at 29, publicly released on May 11, 2017, on *IC on the Record*.

identifiers *not* associated with Section 704 or 705(b) targets that were approved for querying in connection with certain terrorism-related events that occurred in the United States to determine whether these identifiers were improperly queried in Section 702 upstream data. As a result, NSA subsequently determined [redacted] United States person identifiers were improperly queried against upstream data. NSA determined [redacted] improper queries were a result of human error. In addition, [redacted] of the queries were conducted by analysts [redacted]

66 [redacted]

67 [redacted]

68 [redacted]

~~(S//SI//NF)~~ Additionally, NSA's OIG conducted another review of queries – this time of certain known United States person identifiers in Section 702 data for the period of January through March 2016. The OIG found that the root causes of the improper upstream queries it identified through this review were similar to the causes previously identified in the OIG's January 2016 report – analysts had not removed the Section 702 upstream authority from their query criteria or had not included other appropriate limiters to prevent Section 702 upstream data from being queried.

(U) NSA completed a number of actions to address these compliance incidents and has additional actions planned.[70] In September 2016, NSA issued a compliance advisory to its workforce highlighting best practices to avoid non-compliant queries. In late November 2016, NSA issued another compliance advisory to its workforce explaining the relevant query restrictions when querying Section 702 data. In addition, NSA has issued a compliance advisory advising analysts not to use certain systems to conduct queries using known United States person identifiers. NSA also conducted training for analysts and query auditors and provided a compliance advisory to the workforce that requires analysts to include in their query justifications the fact that an identifier is known to be associated with a United States person when that is the case.

(U) NSA has also implemented technical improvements to address this issue. NSA deployed a change to how analysts select Section 702 data in a particular tool. Analysts must now affirmatively select datasets in creating a query. As of December 2016, NSA analysts who are using this tool are required to make an affirmative, conscious decision as to which data sources the query will run against. This change applies to all interfaces in the tool, and NSA is implementing additional technical changes to mitigate this problem. NSA is also deploying technical adjustments to certain frequently used interfaces of this tool that will require analysts to affirmatively specify when their intent is to make a query using a United States person identifier. If an analyst indicates that the intent is to include a U.S. person identifier, these interfaces do not provide the option to query Section 702 upstream data.

---

[70] (U) As a result of this incident and as previously described, the FISC twice extended its examination of the government's application for the 2016 certifications pursuant to 50 U.S.C.§1881a(j)(2). Originally, the 2015 certifications were set to expire on November 6, 2016, but due to the FISC's extensions, the 2015 certification stayed in effect through April 2017, at which time the FISC approved the 2016 certifications. Notice of the extensions were provided to the relevant Congressional committees.

~~(S//NF)~~ In response to this query incident, [redacted] *Thus, NSA no longer acquires communications where the targeted selector is found within the content of a communication, commonly referred to as "abouts" collection.* The government submitted to the FISC revised versions of NSA's Section 702 targeting and minimization procedures to address the above changes to its upstream Internet collection program. NSA also notified the appropriate Congressional committees regarding its changes to its Section 702 upstream Internet collection. The FISC subsequently approved the 2016 certifications in its opinion dated April 26, 2017, concluding that NSA's revised targeting and minimization procedures complied with statutory requirements and were consistent with the Fourth Amendment.

(U) (2) Errors That Can Be Reduced Through System/Process Changes

(U) During this reporting period, one of NSA's tasking errors[71] involved potential non-compliance with the pre-tasking checks required by NSA's Section 702 targeting procedures. NSA's Section 702 targeting procedures require analysts to conduct due diligence to assess whether a target is a non-United States person reasonably believed to be located outside the United States based upon the totality of the circumstances available. In conducting oversight of the Section 702 program, the joint oversight team determined that NSD, ODNI, and NSA have lacked a common understanding of the scope of NSA's pre-tasking checks – i.e., the type of information available to and used by an analyst prior to tasking a facility.

[redacted]

[71] [redacted]

[redacted]

(U) In addition, 12% of detasking delays[72] were caused by NSA's failure to review collection on certain tasked selectors.[73] To address these detasking delays, beginning in April/May of 2016, NSA implemented a change in its tasking tool and designated one group of analysts to review collection for these types of selectors to ensure that collection is reviewed. Significantly, none of these detasking delays involved United States persons.

(U) In prior Joint Assessments, the joint oversight team recommended that certain modifications be made to NSA's querying tool. Specifically, the joint oversight team recommended that:

> NSA assess modifications to systems used to query raw Section 702-acquired data to require analysts to identify when they believe they are using a United States person identifier as a query term. Such an improvement, even if it cannot be adopted universally in all NSA systems, could help prevent compliance instances with respect to the use of United States person query terms.

See The 13th Joint Assessment dated September 2015 at. 41.[74]

(U) The joint oversight team assessed that such an improvement could help prevent compliance instances with respect to the use of United States person query terms. In response to

[redacted]

[74] (U) As previously reported, the U.S. House of Representatives Permanent Select Committee on Intelligence (HPSCI) requested, in a letter dated October 27, 2015, (hereafter the *HPSCI October 2015 letter*) that the Director of National Intelligence submit a report including, among other things, information pertaining to the "status of the proposed changes [DOJ] suggested the [NSA] make to its tasking tool for Section 702 queries" as referenced in the September 2015 Joint Assessment. On February 16, 2016, ODNI provided HPSCI with a report in response to the *HPSCI October 2015 letter*. The ODNI report, *Assessment of Oversight and Compliance with Targeting Procedures* (hereafter the *ODNI February 2016* report), included, among other information, an update on the status of proposed modifications DOJ and ODNI suggested that NSA make to its querying tool. The text above provides a further update.

this recommendation, NSA developed a solution, described above, that involved technical adjustments to certain frequently used interfaces of a commonly used tool for querying certain repositories containing raw Section 702-acquired information that requires analysts to affirmatively specify when their intent is to make a query using a United States person identifier. If an analyst indicates that the intent is to include a U.S. person identifier, these interfaces do not provide the option to query Section 702 upstream data. Although this change does not apply to all NSA systems, NSA assesses that this will assist in reducing compliance incidents, as this is a commonly used tool for querying raw Section 702 information. The prior joint assessment, which noted that NSA had adopted a solution to this recommendation, stated that once the query is executed, the details concerning the query will be passed to NSA's auditing system of record for post-query review and potential metrics compilation and that, as part of the testing, NSA would evaluate the accuracy of reporting this number in future Joint Assessments.[75]

(U) (3) Errors Caused by Misunderstandings of Processes or Procedures That Can Be Addressed Through Training

(U) The joint oversight team identified a number of incidents during this reporting period caused by analysts, officers, or agents misunderstanding or misapplying the requirements of NSA's targeting or minimization procedures. These incidents were attributable, to varying degrees, to a misunderstanding or misapplication of these rules. The joint oversight team assesses that the low overall rate of such incidents and the fact that such incidents are not overly concentrated in any particular area generally reflects the strength of the agencies training program.

~~(TS//SI//NF)~~ For example, in a series of incidents, due to a misunderstanding of the tasking requirements, analysts incorrectly tasked a particular type of facility from a particular provider.[76]

[redacted]

75 [redacted]

76 [redacted]

[redacted] NSA provided guidance to analysts regarding the proper implementation of taskings pursuant to Section 702 for this particular provider to address the above described compliance incidents.

(U) F. Intra- and Inter-Agency Communications

(U) Section 702 compliance requires good communication and coordination within and between agencies. In order to ensure targeting decisions are made based on the totality of the circumstances and after the exercise of due diligence, those involved in the targeting decision must communicate the relevant facts to each other. Analysts also must have access to the necessary records that inform such decisions. Good communication among analysts is also needed to ensure that facilities are promptly detasked when it is determined that the Government has lost its reasonable basis for assessing that the facility is used by a non-United States person reasonably believed to be located outside the United States for the purpose of acquiring foreign intelligence information. Furthermore, query rules regarding United States person identifiers and dissemination decisions regarding United States person information require inter- and intra-agency communications regarding who the Government has determined to be a United States person.

(U) In general, the joint oversight team found that better communication and coordination between and among the agencies reduced certain types of errors from occurring during this reporting period. Still, in this reporting period, miscommunications resulted in errors, and the joint oversight team assesses that there is room for continued improvement: approximately 4% of the detasking delays that occurred were attributable to miscommunications or delays in communicating relevant facts.[77] In addition, 3% of the detasking delays due to intra-agency miscommunication involved United States persons.

[redacted]

[77] [redacted]

[78] [redacted]

(U) The joint oversight team believes that agencies should continue their training efforts to ensure that appropriate protocols continue to be utilized. As part of its on-going oversight efforts, the joint oversight team will also continue to monitor NSA, CIA and FBI's Section 702 activities and practices to ensure that the agencies maintain efficient and effective channels of communication.

(U) III. Review of Compliance Incidents – CIA Minimization Procedures

~~(S//NF)~~ During this reporting period, there were no incidents involving noncompliance with the CIA minimization procedures, which is a decrease from the one incident that occurred in the previous reporting period. [redacted]

(U) IV. Review of Compliance Incidents – FBI Targeting and Minimization Procedures

(U) There were a number of incidents involving noncompliance with the FBI targeting and minimization procedures in this reporting period. As a percentage of FBI's targeting actions during the reporting period, the FBI targeting compliance incident rate during this reporting period increased from almost zero to 0.01%.

~~(S//NF)~~ The minimal number of incidents involving noncompliance with FBI's minimization procedures resulted from misapplication or misunderstanding of the procedures by FBI employees and from technical issues.[79] [redacted],[80] [redacted]

[79] [redacted]

[80] [redacted]

[redacted]

81 [redacted]

82 [redacted]

[redacted]

(U) During this reporting period, there were no minimization errors that involved the improper dissemination of United States person information. The previous joint assessment explained that FBI had recalled five of the seven improper disseminations described in the 14th Joint Assessment[83] and further explained that, at that time, FBI was continuing to discuss the remaining two improper disseminations with NSD.

(U) V. Review of Compliance Incidents – Provider Errors

~~(S//NF)~~ During this reporting period, there were [redacted] incidents (as opposed to no incidents during the last reporting period) of noncompliance by an electronic communication service provider with a Section 702(h) directive. Given that errors by the service providers can result in the acquisition of United States person information, the Government must actively monitor the acquisitions that the providers transmit to the Government. The joint oversight team believes that the historically low number of compliance incidents caused by service providers reflect, in part, the service providers' commitment to comply with the law while protecting their customers' interests. However, the low number of these incidents also reflects continued efforts by the Government and service providers to ensure that lawful intercept systems are effective and compliant with all applicable law and other requirements. The Government must continue to work with the service providers to prevent future incidents of non-compliance.

83 [redacted]

(U) SECTION 5: CONCLUSION

(U) During the reporting period, the joint oversight team found that the agencies have continued to implement the procedures and to follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702. As in previous reporting periods, the joint oversight team has identified no indications of any intentional or willful attempts to violate or circumvent the requirements of the Act in the compliance incidents assessed herein. Although the number of compliance incidents continued to remain small, particularly when compared with the total amount of collection activity, a continued focus is needed to address underlying causes of the incidents which did occur. The joint oversight team assesses that such focus should emphasize maintaining close monitoring of collection activities and continued personnel training. Additionally, as part of its on-going oversight responsibilities, the joint oversight team, and the agencies' internal oversight regimes, will continue to monitor the efficacy of measures to address the causes of compliance incidents during the next reporting period.

APPENDIX A

APPENDIX A

(U) IMPLEMENTATION OF SECTION 702 AUTHORITIES - OVERVIEW

(U) I. Overview - NSA

(U) The National Security Agency (NSA) seeks to acquire foreign intelligence information concerning specific targets under each Section 702 certification from or with the assistance of electronic communication service providers, as defined in Section 701(b)(4) of the Foreign Intelligence Surveillance Act of 1978, as amended (FISA).[1] As required by Section 702, those targets must be non-United States persons[2] reasonably believed to be located outside the United States.

~~(S//NF)~~ During this reporting period, NSA conducted foreign intelligence analysis to identify targets of foreign intelligence interest that fell within one of the following certifications:

[redacted]

[1] (U) Specifically, Section 701(b)(4) provides:

> The term 'electronic communication service provider' means -- (A) a telecommunications carrier, as that term is defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153); (B) a provider of electronic communication service, as that term is defined in section 2510 of title 18, United States Code; (C) a provider of a remote computing service, as that term is defined in section 2711 of title 18, United States Code; (D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; or (E) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), or (D).

[2] (U) Section 101(i) of FISA defines "United States person" as follows:

> a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section101(a)(20) of the Immigration and Nationality Act [8 U.S.C. § 1101(a)(20)]), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3).

[3] [redacted]

[4] [redacted]

(U) As affirmed in affidavits filed with the Foreign Intelligence Surveillance Court (FISC), NSA believes that the non-United States persons reasonably believed to be outside the United States who are targeted under these certifications will either possess foreign intelligence information about the persons, groups, or entities covered by the certifications or are likely to receive or communicate foreign intelligence information concerning these persons, groups, or entities. This requirement is reinforced by the Attorney General's Acquisition Guidelines, which provide that an individual may not be targeted unless a significant purpose of the targeting is to acquire foreign intelligence information that the person possesses, is reasonably expected to receive, and/or is likely to communicate.

(U) Under NSA's FISC-approved targeting procedures, NSA targets a particular non-United States person reasonably believed to be located outside the United States by tasking facilities used by that person who possesses or who is likely to communicate or receive foreign intelligence information. A facility (also known as a "selector") is a specific communications identifier tasked to acquire foreign intelligence information that is to, from, or - under the targeting procedures approved during this assessment's reporting period - about a target. A "facility" could be a telephone number or an identifier related to a form of electronic communication, such as an e-mail address.[5] In order to acquire foreign intelligence information from or with the assistance of an electronic communications service provider, NSA first uses the identification of a facility to acquire the relevant communications. Then, after applying its targeting procedures (further discussed below) and other internal reviews and approvals, NSA "tasks" that facility in the relevant tasking system. The facilities are in turn provided to electronic communication service providers who have been served with the required directives under the certifications.

(U) Once information is collected from these tasked facilities, it is subject to FISC-approved minimization procedures. NSA's minimization procedures set forth specific measures NSA must take when it acquires, retains, and/or disseminates non-publicly available information about United States persons. All collection of Section 702 information is routed to NSA. However, the NSA's minimization procedures also permit the provision of unminimized communications to the Central Intelligence Agency (CIA) and Federal Bureau of Investigation (FBI) relating to targets identified by these agencies that have been the subject of NSA acquisition under the certifications. The unminimized communications sent to CIA and FBI, in accordance with NSA's targeting and minimization procedures, must in turn be processed by CIA and FBI in accordance with their respective FISC-approved Section 702 minimization procedures.[6]

(U) NSA's targeting procedures address, among other subjects, the manner in which NSA will determine that a person targeted under Section 702 is a non-United States person reasonably

---

5 [redacted]

6 [redacted]

believed to be located outside the United States, the post-targeting analysis conducted on the facilities, and the documentation required.

(U) A. Pre-Tasking Location

(U) 1. Telephone Numbers

~~(S//SI//NF)~~ For telephone numbers, NSA analysts [redacted]

(U) 2. Electronic Communications Identifiers

~~(S//SI//NF)~~ For electronic communications identifiers, NSA analysts [redacted]

[7] [redacted]

[8] (U) Analysts also check this system as part of the "post-targeting" analysis described below.

[9] [redacted]

(U) B. Pre-Tasking Determination of United States Person Status

[redacted]

(U) C. Post-Tasking Checks

[redacted]

~~(S//REL TO USA, FVEY)~~ NSA also requires that tasking analysts review information collected from the facilities they have tasked. With respect to NSA's review of [redacted][11] a notification e-mail is sent to the tasking team upon initial collection for the facility. NSA analysts are expected to review this collection within five business days to confirm that the user of the facility is the intended target, that the target remains appropriate to the certification cited, and that the target remains outside the United States. Analysts are then responsible to review traffic on an on-going basis to ensure that the facility remains appropriate under the authority. [redacted] Should traffic not be viewed in at least once every 30 days, a notice is

[10] [redacted]

[11] ~~(S//NF)~~ NSA's automated notification system to ensure analysts have reviewed collection is currently implemented only for [redacted], not [redacted]. NSA is attempting to develop a similar system for [redacted]

sent to the tasking team, as well as to their management, who then have the responsibility to follow up.

(U) D. Documentation

~~(S//NF)~~ The procedures provide that analysts will document in the tasking database a citation to the information leading them to reasonably believe that a targeted person is located outside the United States. The citation is a reference that includes the source of the information, [redacted], enabling oversight personnel to locate and review the information that led the analyst to his/her reasonable belief. Analysts must also identify the foreign power or foreign territory about which they expect the proposed targeting will obtain foreign intelligence information.

~~(S//NF)~~ NSA has [redacted] an existing database tool, for use by its analysts for Section 702 tasking and documentation purposes. [redacted] to assist analysts as they conduct their work. This tool has been modified over time to accommodate the requirements of Section 702, to include, for example, certain fields and features for targeting, documentation, and oversight purposes. Accordingly, the tool allows analysts to document the required citation to NSA records on which NSA relied to form the reasonable belief that the target was located outside the United States. [redacted] The tool has fields for the certification under which the target falls, and for the foreign power as to which the analyst expects to collect foreign intelligence information. Analysts fill out various fields [redacted] each facility, as appropriate, including the citation to the information on which the analyst relied in making the foreignness determination.

(U) NSA's targeting procedures also require analysts to identify the foreign power or foreign territory about which they expect the proposed targeting will obtain foreign intelligence information and provide a written explanation of the basis for their assessment, at the time of targeting, that the target possesses, is expected to receive, and/or is likely to communicate foreign intelligence information concerning that foreign power or foreign territory.

(U) NSA also includes the targeting rationale (TAR) in the tasking record, which requires the targeting analyst to briefly state why targeting for a particular facility was requested. The intent of the TAR is to memorialize why the analyst is requesting targeting, and provides a linkage between the user of the facility and the foreign intelligence purpose covered by the certification under which it is being tasked. The joint oversight team assesses that the TAR has improved the oversight team's ability to understand NSA's foreign intelligence purpose in tasking facilities.

~~(S//NF)~~ [redacted] Entries are reviewed before a tasking can be finalized. Records from this tool are maintained and compiled for oversight purposes. For each facility, a record can be compiled and printed showing certain relevant fields, such as: the facility, the certification, the citation to the record or records relied upon by the analyst, [redacted] the analyst's

foreignness explanation, the targeting rationale, [redacted] These records, referred to as "tasking sheets," are reviewed by the Department of Justice's National Security Division (NSD) and the Office of the Director of National Intelligence (ODNI) as part of the oversight process.

~~(S//NF)~~ The source records cited on these tasking sheets are contained in a variety of NSA data repositories. These records are maintained by NSA and, when requested by the joint team, are produced to verify determinations recorded on the tasking sheets. Other source records may consist of "lead information" from other agencies, such as disseminated intelligence reports or lead information [redacted]

(U) F. Internal Procedures

(U) NSA has instituted internal training programs, access control procedures, standard operating procedures, compliance incident reporting measures, and similar processes to implement the requirements of the targeting procedures. Only analysts who have received certain types of training and authorizations are provided access to the Section 702 program data. These analysts must complete an NSA OGC and Signals Intelligence Directorate (SID) Oversight and Compliance training program; review the targeting and minimization procedures as well as other documents filed with the certifications; and must pass a competency test. The databases NSA analysts use are subject to audit and review by SID Oversight and Compliance. For guidance, analysts consult standard operating procedures, supervisors, SID Oversight and Compliance personnel, NSA OGC attorneys, and the NSA Office of the Director of Compliance.

(U) NSA's targeting and minimization procedures require NSA to report to NSD and ODNI any incidents of non-compliance with the procedures by NSA personnel that result in the intentional targeting of a person reasonably believed to be located in the United States, the intentional targeting of a United States person, or the intentional acquisition of any communication in which the sender and all intended recipients are known at the time of acquisition to be located within the United States, with a requirement to purge from NSA's records any resulting collection. NSA must also report any incidents of non-compliance, including overcollection, by any electronic communication service provider issued a directive under Section 702. Additionally, if NSA learns, after targeting a person reasonably believed to be outside the United States, that the person is inside the United

States, or if NSA learns that a person who NSA reasonably believed was a non-United States person is in fact a United States person, NSA must terminate the acquisition, and treat any acquired communications in accordance with its minimization procedures. In each of the above situations, NSA's Section 702 procedures during this reporting period required NSA to report the incident to NSD and ODNI within the time specified in the applicable targeting procedures (five business days) of learning of the incident.

(U) The NSA targeting and minimization procedures require NSA to conduct oversight activities and make any necessary reports, including those relating to incidents of non-compliance, to the NSA Office of the Inspector General (NSA OIG) and NSA OGC. SID Oversight and Compliance conducts spot checks of targeting decisions and disseminations to ensure compliance with procedures. SID also maintains and updates an NSA internal website regarding the implementation of, and compliance with, the Section 702 authorities.

(U) NSA has established standard operating procedures for incident tracking and reporting to NSD and ODNI. The SID Oversight and Compliance office works with analysts at NSA, and with CIA and FBI points of contact as necessary, to compile incident reports which are forwarded to both the NSA OGC and NSA OIG. NSA OGC then forwards the incidents to NSD and ODNI.

(U) On a more programmatic level, under the guidance and direction of the Office of the Director of Compliance (ODOC), NSA has implemented and maintains a Comprehensive Mission Compliance Program (CMCP) designed to effect verifiable conformance with the laws and policies that afford privacy protection to United States persons during NSA missions. ODOC complements and reinforces the intelligence oversight program of NSA OIG and oversight responsibilities of NSA OGC.

(U) A key component of the CMCP is an effort to manage, organize, and maintain the authorities, policies, and compliance requirements that govern NSA mission activities. This effort, known as "Rules Management," focuses on two key components: (1) the processes necessary to better govern, maintain, and understand the authorities granted to NSA and (2) technological solutions to support (and simplify) Rules Management activities. ODOC also coordinated NSA's use of the Verification of Accuracy (VoA) process originally developed for other FISA programs to provide an increased level of confidence that factual representations to the FISC or other external decision makers are accurate and based on an ongoing, shared understanding among operational, technical, legal, policy and compliance officials within NSA. NSA has also developed a Verification of Interpretation (VoI) review to help ensure that NSA and its external overseers have a shared understanding of key terms in Court orders, minimization procedures, and other documents that govern NSA's FISA activities. ODOC has also developed a risk assessment process to assess the potential risk of non-compliance with the rules designed to protect United States person privacy. The assessment is conducted and reported to the NSA Deputy Director and NSA Senior Leadership Team biannually.

(U) II. Overview - CIA

(U) A. CIA's Role in Targeting

~~(S//NF)~~ Although CIA does not target or acquire communications pursuant to Section 702, CIA has put in place a process, in consultation with NSA, FBI, NSD, and ODNI, to identify foreign intelligence targets to NSA (hereinafter referred to as the "CIA nomination process"). Based on its foreign intelligence analysis, CIA may "nominate" a facility to NSA for potential acquisition under one of the Section 702(g) certifications. [redacted] Nominations are reviewed and approved by a targeting officer's first line manager, a component legal offic[redacted]

[redacted]

[12] [redacted]

~~(S//NF)~~ The FISA Program Office was established in December 2010 [redacted] and is charged with providing strategic direction for the management and oversight of CIA's FISA collection programs, including the retention and dissemination of foreign intelligence information acquired pursuant to Section 702. This group is responsible for overall strategic direction and policy, programmatic external focus, and interaction with counterparts of NSD, ODNI, NSA and FBI. In addition, the office leads the day-to-day FISA compliance efforts [redacted] The primary responsibilities of the FISA Program Office are to provide strategic direction for data handling and management of FISA/702 data, as well as to ensure that all Section 702 collection is properly tasked and that CIA is complying with all compliance and purge requirements.

(U) B. Oversight and Compliance

(U) CIA's FISA compliance program is managed by its FISA Program Office in coordination with CIA OGC. CIA provides small group training to personnel who nominate facilities to NSA and/or minimize Section 702-acquired communications. Access to unminimized Section 702-acquired communications is limited to trained personnel. CIA attorneys embedded with operational elements that have access to unminimized Section 702-acquired information also respond to inquiries regarding nomination and minimization questions. Identified incidents of noncompliance with the CIA minimization procedures are generally reported to NSD and ODNI by CIA OGC.

(U) III. Overview - FBI

(U) A. FBI's Role in Targeting – Nomination for Acquiring [redacted] Communications

~~(S//NF)~~ Like CIA, FBI has developed a formal nomination process to identify foreign intelligence targets to NSA for the acquisition of [redacted] communications. [redacted] including information underlying the basis for the foreignness determination and the foreign intelligence interest. FBI nominations are reviewed by FBI operational and legal personnel prior to export to NSA for tasking. [redacted] The FBI targeting procedures require that NSA first apply its own targeting procedures to determine that the user of the Designated Account is a person reasonably believed to be outside the United States and is not a

United States person. NSA is also responsible for determining that a significant purpose of the acquisition it requests is to obtain foreign intelligence information. After NSA designates accounts as being appropriate [redacted], FBI must then apply its own, additional procedures, which require FBI to review NSA's conclusion of foreignness [redacted]

~~(S//NF)~~ More specifically, after FBI obtains the tasking sheet from NSA, it reviews the information provided by NSA regarding the location of the person and the non-United States person status of the person. [redacted]

[redacted]

~~(S//NF)~~ Unless FBI locates information indicating that the user is a United States person or is located inside the United States, FBI will [redacted]

~~(S//NF)~~ If FBI identifies information indicating that NSA's determination that the target is a non-United States person reasonably believed to be outside the United States may be incorrect, FBI provides this information to NSA and does not approve [redacted]

(U) C. Documentation

~~(S//NF)~~ The targeting procedures require that FBI retain the information [redacted] in accordance with its records retention policies a[redacted]. FBI uses a multi-page checklist for each Designated Account to record the results of its targeting process, as laid out in its standard operating procedures, commencing with [redacted], extending through [redacted] nd culminating in approval or disapproval of the acquisition. In addition, the FBI standard operating procedures call for [redacted] depending on the circumstances, which are maintained by FBI with the applicable checklist. FBI also retains with each checklist any relevant communications [redacted] regarding its review of the [redacted] information. Additional checklists have been created to capture information on requests withdrawn [redacted] or not approved by FBI.

(U) D. Implementation, Oversight, and Compliance

~~(S//NF)~~ FBI's implementation and compliance activities are overseen by FBI OGC, particularly the National Security Law Branch (NSLB), as well as FBI's Exploitation Threat Section (XTS), [redacted]), and FBI's Inspection Division (INSD). [redacted] XTS has the lead responsibility in FBI for [redacted] requests [redacted]. XTS personnel are trained on the FBI targeting procedures and FBI's detailed set of standard operating procedures that govern its processing of requests [redacted]. XTS also has the lead responsibility for facilitating FBI's nominations to NSA [redacted] communications. XTS, NSLB, NSD, and ODNI have all worked on training FBI personnel to

ensure that FBI nominations and post-tasking review comply with the NSA targeting procedures. Numerous such trainings were provided during the current reporting period. With respect to minimization, FBI has created a mandatory online training that all FBI agents and analysts must complete prior to gaining access to unminimized Section 702-acquired data in the FBI's [redacted] In addition, NSD conducts training on the Section 702 minimization Procedures at multiple FBI field offices each year.

~~(S//NF)~~ The FBI's targeting procedures require periodic reviews by NSD and ODNI at least once every 60 days. FBI must also report incidents of non-compliance with the FBI targeting procedures to NSD and ODNI within five business days of learning of the incident. XTS and NSLB are the lead FBI elements in ensuring that NSD and ODNI received all appropriate information with regard to these two requirements.

(U) IV. Overview - Minimization

(U) Once a facility has been tasked for collection, non-publicly available information collected as a result of these taskings that concerns United States persons must be minimized. The FISC-approved minimization procedures require such minimization in the acquisition, retention, and dissemination of foreign intelligence information. As a general matter, minimization procedures under Section 702 are similar in most respects to minimization under other FISA orders. For example, the Section 702 minimization procedures, like those under certain other FISA court orders, allow for sharing of certain unminimized Section 702 information among NSA, FBI, and CIA. Similarly, the procedures for each agency require special handling of intercepted communications that are between attorneys and clients, as well as foreign intelligence information concerning United States persons that is disseminated to foreign governments.

(U) The minimization procedures do, however, impose additional obligations or restrictions as compared to minimization procedures associated with authorities granted under Titles I and III of FISA. For example, the Section 702 minimization procedures require, with limited exceptions, the purge of any communications acquired through the targeting of a person who at the time of targeting was reasonably believed to be a non-United States person located outside the United States, but is in fact located inside the United States at the time the communication is acquired, or was in fact a United States person at the time of targeting.

(U) NSA, CIA, and FBI have created systems to track the purging of information from their systems. CIA and FBI receive incident notifications from NSA to document when NSA has identified Section 702 information that NSA is required to purge according to its procedures, so that CIA and FBI can meet their respective obligations.